United States Department of State

Bureau for International Narcotics and Law Enforcement Affairs

International Narcotics Control Strategy Report

Volume II

Money Laundering and Financial Crimes

March 2009

Table of Contents
Volume II

Common Abbreviations vi
Legislative Basis for the INCSR 3
Introduction 4
Growing Threats 4
Extant Challenges 7
Bilateral Activities 9
Training and Technical Assistance 9
Department of State 9
International Law Enforcement Academies (ILEAs) 11
Board of Governors of the Federal Reserve System (FRB) 13
Federal Bureau of Investigation (FBI), Department of Justice 14
Federal Deposit Insurance Corporation (FDIC) 15
Financial Crimes Enforcement Network (FinCEN), Department of Treasury 15
Immigration and Customs Enforcement, Department of Homeland Security (DHS) 17
Bulk Cash Smuggling 17
Trade Transparency Units (TTUs) 18
Other ICE Programs 18
Internal Revenue Service (IRS), Criminal Investigative Division (CID) Department of Treasury 18
Office of the Comptroller of the Currency (OCC), Department of Treasury 19
Office of Overseas Prosecutorial Development, Assistance and Training, the Asset Forfeiture and Money Laundering Section, & Counterterrorism Section (OPDAT, AFMLS, and CTS), Department of Justice 20
Training and Technical Assistance 20
Money Laundering/Asset Forfeiture/Fraud 21
Terrorism/Terrorist Financing 26
Office of Technical Assistance (OTA), Treasury Department 28
Assessing Training and Technical Assistance Needs 29
AML/CTF Training 29
Financial Intelligence Units 31
Casinos and Gaming 31
Insurance 32
Regional and Resident Advisors (RA) 32
Treaties and Agreements 33
Treaties 33
Agreements 33
Asset Sharing 34
Multi-Lateral Organizations & Programs 34
The Financial Action Task Force (FATF) and FATF-Style Regional Bodies (FSRBs) 34
The Financial Action Task Force (FATF) 34
The Asia Pacific Group (APG) 35
The Caribbean Financial Action Task Force (CFATF) 35

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) 35
The Eastern and South African Anti Money Laundering Group (ESAAMLG) 35
The Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) 36
The Financial Action Task Force on Money Laundering in South America (GAFISUD) 36
The Groupe Intergouvernemental d'Action contre le Blanchiment en Afrique/ Intergovernmental Action Group against Money Laundering in West Africa (GIABA) 36
The Middle East and North Africa Financial Action Task Force (MENAFATF) 36

The Egmont Group of Financial Intelligence Units 36

The Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Group of Experts to Control Money Laundering 38

Pacific Anti-Money Laundering Program (PALP) 39
Mentoring 40
Legislative Drafting 40
Capacity Building Initiatives 41
Civil Forfeiture 42
Case Support 42
The Year Ahead 42

United Nations Global Programme Against Money Laundering 43
The Mentoring Program 43
Mentoring and FIUs 44
Computer-Based Training 44
Other GPML Initiatives 45

Law Enforcement Cases 46
Lloyds of London Violates IEEPA 46
Holy Land Foundation Revisited 47
Hawala, Money Laundering and Terrorism Financing 47
NGO Support of a Terror Organization 48
"Bust-Out" Scheme 48
Sentencing Hearings Held in CARE International Case 48
Money Laundering and Harboring Illegal Aliens 49

Major Money Laundering Countries 49

Vulnerability Factors 51

Changes in INCSR Priorities for 2008 52

Country/Jurisdiction Table 53

Introduction to Comparative Table 54

Glossary of Terms 54

Comparative Table 56

Country Reports 65
Afghanistan 65
Albania 69
Algeria 72
Angola 74
Antigua and Barbuda 75
Argentina 79
Aruba 83
Australia 85
Austria 91
Azerbaijan 94
Bahamas 98
Bahrain 101

Bangladesh 105
Barbados 109
Belarus 111
Belgium 116
Belize 121
Bolivia 125
Bosnia and Herzegovina 128
Brazil 133
British Virgin Islands 137
Bulgaria 141
Burma 146
Cambodia 149
Canada 152
Cayman Islands 156
Chile 159
China, People's Republic of 165
Colombia 170
Comoros 175
Cook Islands 178
Costa Rica 181
Côte d'Ivoire 184
Cyprus 188
Czech Republic 195
Dominican Republic 199
Ecuador 203
Egypt, The Arab Republic of 206
El Salvador 210
France 212
Germany 215
Ghana 218
Gibraltar 221
Greece 223
Grenada 229
Guatemala 231
Guernsey 236
Guinea-Bissau 238
Guyana 241
Haiti 243
Honduras 245
Hong Kong 250
Hungary 256
India 260
Indonesia 266
Iran 273
Iraq 277
Ireland 281
Isle of Man 284
Israel 287
Italy 292
Jamaica 296
Japan 299
Jersey 303
Jordan 306
Kenya 313
Korea, Democratic Peoples Republic of 316
Korea, Republic of 317

Kuwait 321
Laos 325
Latvia 327
Lebanon 332
Liechtenstein 336
Luxembourg 339
Macau 343
Malaysia 348
Mexico 352
Moldova 358
Monaco 363
Morocco 366
The Netherlands 367
Netherlands Antilles 373
Nicaragua 377
Nigeria 380
Pakistan 384
Palau 388
Panama 392
Paraguay 397
Peru 401
Philippines 405
Poland 410
Portugal 414
Qatar 417
Romania 421
Russia 426
Samoa 431
Saudi Arabia 433
Senegal 436
Serbia 439
Seychelles 443
Sierra Leone 446
Singapore 448
Slovak Republic 453
South Africa 457
Spain 459
St. Kitts and Nevis 465
St. Lucia 468
St. Vincent and the Grenadines 470
Suriname 472
Switzerland 476
Syria 480
Taiwan 485
Tanzania 490
Thailand 491
Trinidad and Tobago 496
Turkey 499
Turks and Caicos 503
Ukraine 506
United Arab Emirates 511
United Kingdom 518
Uruguay 522
Uzbekistan 526
Vanuatu 531
Venezuela 535

Vietnam 538
Yemen 541
Zimbabwe 544

Common Abbreviations

AML	Anti-Money Laundering
APG	Asia/Pacific Group on Money Laundering
ARS	Alternative Remittance System
BCS	Bulk Cash Smuggling
CFATF	Caribbean Financial Action Task Force
CTF	Counterterrorist Financing
CTR	Currency Transaction Report
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOJ	Department of Justice
DOS	Department of State
EAG	Eurasian Group to Combat Money Laundering and Terrorist Financing
EC	European Commission
ECOWAS	Economic Community of West African States
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
EU	European Union
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FinCEN	Financial Crimes Enforcement Network
FIU	Financial Intelligence Unit
FSRB	FATF-Style Regional Body
GAFISUD	Financial Action Task Force on Money Laundering in South America
GIABA	Inter-Governmental Action Group against Money Laundering
IBC	International Business Company
ICE	U.S. Immigration and Customs Enforcement
IFI	International Financial Institution
IMF	International Monetary Fund
INCSR	International Narcotics Control Strategy Report
INL	Bureau for International Narcotics and Law Enforcement Affairs
IRS	Internal Revenue Service
IRS-CID	Internal Revenue Service, Criminal Investigative Division
IVTS	Informal Value Transfer System
MENAFATF	Middle East and North Africa Financial Action Task Force
MLAT	Mutual Legal Assistance Treaty
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
MOU	Memorandum of Understanding
NCCT	Non-Cooperative Countries or Territories
NGO	Non-Governmental Organization
NPO	Non-Profit Organization
OAS	Organization of American States
OAS/CICAD	OAS Inter-American Drug Abuse Control Commission
OFAC	Office of Foreign Assets Control

Common Abbreviations (Continued)

OFC	Offshore Financial Center
OPDAT	Office of Overseas Prosecutorial Development, Assistance and Training
OTA	Office of Technical Assistance
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TBML	Trade-Based Money Laundering
TTU	Trade Transparency Unit
UNCAC	United Nations Convention against Corruption
UN Drug Convention	1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances
UNGPML	United Nations Global Programme against Money Laundering
UNODC	United Nations Office for Drug Control and Crime Prevention
UNSCR	United Nations Security Council Resolution
UNTOC	United Nations Convention against Transnational Organized Crime
USAID	Agency for International Development
USG	United States Government

MONEY LAUNDERING AND FINANCIAL CRIMES

Legislative Basis for the INCSR

The Money Laundering and Financial Crimes section of the Department of State's International Narcotics Control Strategy Report (INCSR) has been prepared in accordance with section 489 of the Foreign Assistance Act of 1961, as amended (the "FAA," 22 U.S.C. § 2291). The 2009 INCSR is the 26th annual report prepared pursuant to the FAA.[1]

The FAA requires a report on the extent to which each country or entity that received assistance under chapter 8 of Part I of the Foreign Assistance Act in the past two fiscal years has "met the goals and objectives of the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances" (the "1988 UN Drug Convention")(FAA § 489(a)(1)(A)).

Although the Convention does not contain a list of goals and objectives, it does set forth a number of obligations that the parties agree to undertake. Generally speaking, it requires the parties to take legal measures to outlaw and punish all forms of illicit drug production, trafficking, and drug money laundering, to control chemicals that can be used to process illicit drugs, and to cooperate in international efforts to these ends. The statute lists action by foreign countries on the following issues as relevant to evaluating performance under the 1988 UN Drug Convention: illicit cultivation, production, distribution, sale, transport and financing, money laundering, asset seizure, extradition, mutual legal assistance, law enforcement and transit cooperation, precursor chemical control, and demand reduction.

In attempting to evaluate whether countries and certain entities are meeting the goals and objectives of the 1988 UN Drug Convention, the Department has used the best information it has available. The 2009 INCSR covers countries that range from major drug producing and drug-transit countries, where drug control is a critical element of national policy, to small countries or entities where drug issues or the capacity to deal with them are minimal. In addition to identifying countries as major sources of precursor chemicals used in the production of illicit narcotics, the INCSR is mandated to identify major money laundering countries (FAA §489(a)(3)(C)). The INCSR is also required to report findings on each country's adoption of laws and regulations to prevent narcotics-related money laundering (FAA §489(a)(7)(C)). This report is the section of the INCSR that reports on money laundering and financial crimes.

A major money laundering country is defined by statute as one "whose financial institutions engage in currency transactions involving significant amounts of proceeds from international narcotics trafficking" (FAA § 481(e)(7)). However, the complex nature of money laundering transactions today makes it difficult in many cases to distinguish the proceeds of narcotics trafficking from the proceeds of other serious crime. Moreover, financial institutions engaging in transactions involving significant

[1] The 2009 report on Money Laundering and Financial Crimes is a legislatively mandated section of the U.S. Department of State's annual International Narcotics Control Strategy Report. This 2009 report on Money Laundering and Financial Crimes is based upon the contributions of numerous U.S. Government agencies and international sources. A principal contributor is the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN), which, as a member of the international Egmont Group of Financial Intelligence Units, has unique strategic and tactical perspective on international anti-money laundering developments. FinCEN is the primary contributor to the individual country reports. Another key contributor is the U.S. Department of Justice's Asset Forfeiture and Money Laundering Section (AFMLS) of Justice's Criminal Division, which plays a central role in constructing the Money Laundering and Financial Crimes Comparative Table and provides international training. Many other agencies also provided information on international training as well as technical and other assistance, including the following: Department of Homeland Security's Bureau of Immigration and Customs Enforcement; Department of Justice's Drug Enforcement Administration, Federal Bureau of Investigation, and Office for Overseas Prosecutorial Development Assistance; and Treasury's Internal Revenue Service, the Office of the Comptroller of the Currency, and the Office of Technical Assistance. Also providing information on training and technical assistance are the independent regulatory agencies, Federal Deposit Insurance Corporation, and the Federal Reserve Board.

amounts of proceeds of other serious crime are vulnerable to narcotics-related money laundering. This year's list of major money laundering countries recognizes this relationship by including all countries and other jurisdictions whose financial institutions engage in transactions involving significant amounts of proceeds from all serious crime. The following countries/jurisdictions have been identified this year in this category:

Major Money Laundering Countries in 2008:

Afghanistan, Antigua and Barbuda, Australia, Austria, Bahamas, Belize, Bolivia, Brazil, Burma, Cambodia, Canada, Cayman Islands, China, Colombia, Costa Rica, Cyprus, Dominican Republic, France, Germany, Greece, Guatemala, Guernsey, Guinea-Bissau, Haiti, Hong Kong, India, Indonesia, Iran, Isle of Man, Israel, Italy, Japan, Jersey, Kenya, Latvia, Lebanon, Liechtenstein, Luxembourg, Macau, Mexico, Netherlands, Nigeria, Pakistan, Panama, Paraguay, Philippines, Russia, Singapore, Spain, Switzerland, Taiwan, Thailand, Turkey, Ukraine, United Arab Emirates, United Kingdom, United States, Uruguay, Venezuela, and Zimbabwe.

The Money Laundering and Financial Crimes section provides further information on these countries/entities, as required by section 489 of the FAA.

Introduction

Volume II of the *2009 International Narcotics Control Strategy Report, Money Laundering and Financial Crimes*, highlights the continuing vulnerabilities and potential threats to stability and security posed by global money laundering, terrorist finance, and other financial crimes. This year's report demonstrates anew that criminals and terrorists continue to disguise their illicit financial activities. Tainted funds have the potential to destabilize economies, weaken the integrity of the international financial system, subvert rules-based international commerce, and corrupt governments. New and cutting edge money laundering methodologies represent tremendous challenges for the financial, regulatory, legal, intelligence, and law enforcement communities.

Earlier editions of this volume have chronicled progress made in formulating and implementing anti-money laundering and counterterrorist financing (AML/CTF) measures. The 2009 INCSR describes recent AML/CTF developments, as well as emerging trends that could merit increased attention.

Growing Threats

Threat Convergence of Illicit Drug Wealth, Organized Crime, and Terrorism. In 2008, Khan Mohammed became the first known Taliban to be convicted of drug trafficking. His case demonstrates the linkages between the proceeds of narcotics, organized crime, and terrorism. In a groundbreaking operation by the U.S. Drug Enforcement Administration, an Afghan farmer acting in an undercover capacity secretly recorded Mohammed conspiring to purchase weapons and engage in trafficking narcotics. Mohammed was arrested and, with the cooperation of the Afghan government, brought to the United States for trial in late 2007. In December 2008, Mohammed was sentenced in U.S. District Court for the District of Columbia to two terms of life in prison on drug trafficking and narcotics terrorism charges.

Afghanistan produces more than 90 per cent of the world's opium. As is discussed below, in this volume's Afghanistan country report, much of the narcotics trade is facilitated by the Taliban. The profits generated by the drug trade enable the Taliban to operate not only in Afghanistan but across parts of Central Asia and Pakistan. Drug terror-threat convergence is also found in Colombia with the Revolutionary Armed Forces of Colombia (FARC), and in Peru with the Sendero Luminoso (Shining

Path). In fact, approximately half the 44 U.S. Department of State designated Foreign Terrorist Organizations have ties to narcotics trafficking.

Trade-Based Money Laundering (TBML). As is made clear in many of the 2009 country reports, trade is used to launder money and transfer value around the world. Estimates of the annual dollar amount laundered through trade range into the hundreds of billions. Some academics have argued that TBML is the most prevalent form of money laundering in the United States. In recent years, analysts and policy makers are increasingly recognizing the existence of trade-based money laundering.

The 2003 edition of this volume introduced the TBML concept. In 2007, TBML was included as a priority threat in the 2007 National Money Laundering Strategy. In recent years, the Financial Action Task Force (FATF) has begun to recognize the need to formulate international countermeasures to address TBML and in June 2008, the FATF produced a best practices paper on the subject. The FATF could emphasize its importance by adding TBML as its tenth "Special Recommendation on Terrorist Financing". The Wolfsberg Group, an association of 12 of the world's largest banks, calls for enhanced due diligence to prevent TBML tied to drug cartels, terrorist organizations, sanctions violators and weapons proliferators. Also, a nascent but growing network of Trade Transparency Units (TTUs) has revealed the extent of transnational TBML through the monitoring of import and export documentation. The United States established a TTU within the U.S. Department of Homeland Security Bureau of Immigration and Customs Enforcement (ICE) that generates both domestic and international investigations. The number of cases initiated by the INL-funded TTU network continues to grow. In 2008, Mexico's TTU investigated seven cases; Colombia, four; Paraguay, six; Brazil, one; and Argentina, two. Unfortunately, financial institutions' compliance programs and corresponding suspicious transaction reporting—which are the backbone of most countries' AML/CTF regimes—are not yet structured fully to detect TBML.

Service-Based Laundering. Just as TBML depends primarily on commodity invoice fraud (particularly over-and-under invoicing), a similar mechanism is used in service-based industries to launder money and illegally transfer funds across borders without detection. Marketing surveys, accounting and legal services, and concert promotions are just a few examples of service-based industries that can conceal international fraud. Fraudulent invoices and supporting documentation can be used to justify payment or the transfer of money for real or fictitious services from one jurisdiction to another. In this manner, some service-based industries may be laundering money, evading taxes, engaging in fraud, and conducting other financial crimes. Pursuing service-based fraud and money laundering is a challenge because there is no commodity to follow. Moreover, investigations are often stymied because law enforcement agencies have difficulties sorting out jurisdictional issues.

Mobile Payments and Stored Value Cards Laundering. The potential threat of mobile payments for money laundering and other financial crimes was highlighted in the 2008 edition of the INCSR. In the digital age, it is increasingly difficult to "follow the money;" and some argue that money launderers and terrorist financiers may attempt to exploit mobile payments. FATF calls mobile payments "new payment methods" or NPMs. They are also sometimes called "e-money" or "digital cash." Examples include Internet payment services, digital precious metals, electronic purses, and mobile payments or "m-payments." Driven by the convergence of the financial and telecommunications sectors, the rapid global growth of m-payments raises particular concern. M-payments can take many forms but are commonly point of sale payments made through a mobile device such as a cellular phone, a smart phone, or a personal digital assistant (PDA).

A related risk is the growing threat from stored value cards (SVCs) as a mechanism for money laundering and terrorist financing. SVCs are cards with data encoded in either a magnetic strip or a computer chip, for example, prepaid credit cards, or gift cards, that are preloaded with a fixed amount of electronic currency or value. The SVCs can be redeemed or transferred to individuals and/or merchants in a manner similar to spending physical currency. An ICE/Internal Revenue Service

investigation into a stolen credit card number network operating in Mexico found that a co-conspirator was paid by a criminal organization with gift cards issued by U.S. retailers. The gift cards were then used to purchase mobile phone cards, which were smuggled into Mexico and sold at a profit. SVCs also pose a challenge in detection, since they fit in a wallet and look like any other plastic card. As we noted in 2008, much work and creative thinking will be necessary to prevent exploitation and misuse of SVCs by money launderers and terrorist financiers while simultaneously maintaining the advantages they offer and protecting both user privacy and the integrity of the global financial system.

Virtual World Laundering. Virtual reality universe games are increasingly popular around the world. Some of these cyberspace games are not just a source of entertainment but a venue for real commercial activity. Players buy and sell virtual property, goods and services. Some games also allow players to convert genuine currency deposits to virtual currency and then back to real currency at fixed exchange rates. Such capabilities in virtual world games have potential implications for money laundering and other financial crimes. It is now possible to set up an account by furnishing false identification, fund the account with illicit proceeds, and have a co-conspirator in a criminal enterprise on the other side of the world withdraw funds. For example, in 2008 South Korean authorities arrested a group involved with the laundering of $38 million in virtual currencies. Observers also fear that terrorist groups may use virtual worlds to meet, chat, plan activities, and perhaps transfer funds. The added venue and jurisdictional challenges of following virtual money and value trails in and out of the virtual world compound the challenges regulatory and law enforcement agencies already face in the real world.

Suspect Internet Value Transfer. The Internet is being used today by money launderers in a variety of ways including Internet gaming and the misuse of on-line payment providers. Some suspect Internet value transfer services avoid financial transparency reporting requirements and other standard regulatory and law enforcement countermeasures. There have been instances where terrorist fundraisers have directed that “contributions” be made via suspect on-line payment providers.

On-line payment providers serve as an electronic alternative to traditional paper settlement methods such as cash, checks and money orders. They connect subscribers, card holders, on-and-offline resellers, as well as online businesses and traditional merchants. For some providers, U.S. dollar-based money can be sent to anyone that has a valid email address, whether or not that address is a subscriber. In the United States, these payment providers are subject to many of the rules and regulations governing nonbank financial institutions and they are registered and licensed as a money service business. However, this is not the case in many jurisdictions, and even where regulations do exist, they are difficult to enforce. Due diligence and “know your customer” requirements often do not exist for online gaming and online payment providers. Users can add credit to their accounts via bank payments. Banks in some countries will transfer money directly into payment provider accounts. Users can also use Internet banking to make transfers directly from any computer. Credit card payments are accepted. And for those who do not wish to use banks, a user can purchase “refill coupons” at a variety of brick and mortar retailers. The nexus of Internet, value transfer, and Internet auctions is a more difficult to detect, virtual mirror to traditional TBML.

Growing Linkage Between Tax Evasion and Money Laundering. According to the Internal Revenue Service (IRS), “Money laundering is the means by which criminals evade paying taxes on illegal income by concealing the source and the amount of profit. Money laundering is in effect tax evasion in progress.” For investigators, separating money laundering from tax evasion is increasingly difficult. Although the intent differs, many of the same methodologies are used. One citizen’s tax haven can be the same as a money launderer’s hidden offshore account. For example, because of the difficulty in determining the true beneficial owners of international business companies (IBCs), they are favored mechanisms to both launder illicit proceeds and evade taxes. As noted in the country reports, the British Virgin Islands and Hong Kong each have nearly 500,000 international business companies (IBCs) registered in their jurisdictions.

Extant Challenges

Lack of Capacity Among Some of the Most Vulnerable Countries. While most countries in the world have committed themselves to upholding the FATF standards, there are many countries that find themselves unable to construct comprehensive AML/CTF regimes, precluding effective implementation. There is often a lack of public understanding about money laundering and financial crimes. Additionally, those charged with monitoring, inspecting, regulating, investigating, and prosecuting violations may suffer a lack of resources that could contribute to inadequate training, and competition for scarce resources. In some countries, systemic corruption also serves as an impediment to the development and implementation of viable anti-money laundering/counterterrorist financing regimes.

Lack of Money Laundering and Terrorist Financing Prosecutions and Convictions. A review of country reports shows that far too many countries that boast solid AML/CTF standards and infrastructures do not enforce their laws. This is true in all corners of the world and for both developed and developing countries alike. In many instances, the lack of enforcement is due to lack of capacity, but in some cases it is due to a lack of political will. The country reports in this INCSR volume document how countries are making progress in enacting enabling legislation and refining reporting requirements that financial institutions, money service businesses, and even nonfinancial businesses must follow to file suspicious transaction reports (STRs)—but the implementation of these measures is stymied. An AML/CTF legal framework, promulgating regulations, the number of STRs filed, and the creation of financial intelligence units (FIUs) are closely tracked metrics. However, there are limited corresponding increases in prosecutions and convictions—the true measure of success.

A review of the 2009 country reports indicates both progress and challenges continue to exist in combating money laundering, terrorist financing, and other financial crimes. The following examples illustrate advances and regression:

- By December 2008, 180 countries had criminalized money laundering to include predicate crimes beyond narcotics- an increase of 17 countries since 2004.
- In 2008, 13 countries criminalized terrorist financing bringing the total to 149 countries that have criminalized terrorist financing—an increase of 36 countries since 2003.
- In Paraguay, the General Attorney's Office processed 40 money laundering cases that resulted in 15 convictions.
- Ghana passed its first anti-money laundering law.
- The FIUs of Moldova and the Turks and Caicos became members of the Egmont Group. Total Egmont membership now totals 107.
- In December, the Egmont Group expelled Bolivia's FIU because of the Bolivian government's refusal to criminalize terrorist financing.
- With approximately 600 money laundering convictions annually, Italy ranks second to only the United States in successful prosecutions.
- In Iran, the Islamic Parliament and Guardian Council approved a new Iranian money laundering law. The law, however, lacks specificity and does not adhere to international standards.
- Serbia adopted a new National Strategy Against Money Laundering and Terrorism Financing.
- Cote d'Ivoire's FIU became operational.

- Russia's FIU estimates that Russian citizens may have laundered as much as $370 billion in 2008.
- The Hungarian FIU seized over 4.5 million euros (approximately $5,694,850) in illicit proceeds, and froze a total of 7 million euros (approximately $8.850,500).
- The Government of Mexico took on internal corruption in 2008 and launched "Operation Clean House" aimed at ending corruption inside its enforcement agencies. By December, eight enforcement agents had been apprehended and accused of leaking confidential information to drug cartels.
- In Indonesia, the scale of the terrorism threat is evidenced by 423 arrests and 367 convictions of terrorists in recent years. However, there has been little success in following the terrorists' money trail and no prosecutions focused on the financing of terrorism.
- In 2008, substantial property assets were seized relating to a Miami, Florida Medicare fraud scandal involving the Benitez brothers. Of the $110 million in fraudulent funds seized, over $30 million were invested in assets in the Dominican Republic.
- In June, Spanish authorities dismantled an international criminal organization accused of drug-related money laundering and cocaine smuggling operations, arresting 21 individuals including nationals of Spain, Colombia, Peru, and Romania.
- In September, Germany participated in a multi-national customs cash smuggling enforcement operation that included many of the European Union countries as well as a number of North African nations. Frankfurt-based representatives of the U.S. Department of Homeland Security Bureau of Immigration and Customs Enforcement (ICE) assisted in the coordination of the operation by providing real-time intelligence support to the German command center. During the week-long effort, 181 cases of money smuggling were discovered and 5.5 million euros (approximately $6,960,250) were seized.
- In Panama, approximately 46,178 IBCs were registered in Panama in 2007 and 40,825 through the first ten months of 2008. Panama has no requirement to disclose the beneficial owners of any corporation or trust; bearer shares are permitted for corporations; and nominee directors and trustees are allowed. The result is that illicit funds can be laundered and taxes evaded with little fear of detection and prosecution.
- The Dominican Republic, Grenada, Jamaica, Trinidad and Tobago plan to open "international financial centers", most of which offer the same services as offshore financial centers.
- In India, the analysis of suspicious transaction reports by the FIU led to the arrest of several suspected terror operatives not involved in the Mumbai attack.
- The European Commission referred Spain, Poland, Belgium and France to the European Court of Justice over non-implementation of the Third Money Laundering Directive, which requires members to update their AML regimes to comport with the most current international standards, particularly with regard to regulation and terrorism financing. The deadline for transposition of the Directive was December 15, 2007.
- Kazakhstan authorities initiated 54 money laundering cases in 2007; 41 were prosecuted, resulting in eight convictions. Kazakhstan estimated that approximately

$400 million was "lost to corruption." In 2008, 21 money laundering cases were successfully prosecuted. Kazakhstan estimated $1.6 billion was lost to corruption.

As history demonstrates again and again, political stability, democracy and free markets depend on solvent, stable, and honest financial, commercial, and trade systems. The Department of State's Bureau of International Narcotics and Law Enforcement Affairs looks forward to continuing to work with our U.S. and international partners in furthering this important work and strengthening capacities globally to combat money laundering and expose the illicit networks of criminal organizations, the web of corruption, and help unravel conspiracies to commit terror acts.

Bilateral Activities

Training and Technical Assistance

During 2008, a number of U.S. law enforcement and regulatory agencies provided training and technical assistance on money laundering countermeasures and financial investigations to their counterparts around the globe. These courses have been designed to give financial investigators, bank regulators, and prosecutors the necessary tools to recognize, investigate, and prosecute money laundering, financial crimes, terrorist financing, and related criminal activity. Courses have been provided in the United States as well as in the jurisdictions where the programs are targeted.

Department of State

The U.S. Department of State's Bureau of International Narcotics and Law Enforcement (INL) Crime Programs Division helps strengthen criminal justice systems and the abilities of law enforcement agencies around the world to combat transnational criminal threats before they extend beyond their borders and impact our homeland. Through its international programs, as well as in coordination with other INL offices and U.S. Government (USG) agencies, the INL Crime Programs Division addresses a broad cross-section of law enforcement and criminal justice sector areas including: counternarcotics; drug demand reduction; money laundering; financial crime; terrorist financing; smuggling of goods; illegal migration; trafficking in persons; domestic violence; border controls; document security; corruption; cyber-crime; intellectual property rights; law enforcement; police academy development; and assistance to judiciaries and prosecutors.

INL and the State Department's Office of the Coordinator for Counterterrorism (S/CT) co-chair the interagency Terrorist Finance Working Group (TFWG), and together are implementing a multi-million dollar training and technical assistance program designed to develop or enhance the capacity of a selected group of more than two dozen countries whose financial sectors have been used, or are vulnerable to being used, to finance terrorism. As is the case with the more than 100 other countries to which INL-funded training was delivered in 2008, the capacity to thwart the funding of terrorism is dependent on the development of a robust anti-money laundering regime. Supported by and in coordination with the U.S. Department of State, U.S. Department of Justice (DOJ), U.S. Department of Homeland Security (DHS), U.S. Department of the Treasury, the Federal Deposit Insurance Corporation, and various nongovernmental organizations, TFWG provided in 2008 a variety of law enforcement, regulatory and criminal justice programs worldwide. This integrated approach includes assistance with the drafting of legislation and regulations that comport with international standards, the training of law enforcement, the judiciary and bank regulators, as well as the development of financial intelligence units (FIUs) capable of collecting, analyzing, and disseminating financial information to foreign analogs. Courses have been provided in the United States as well as in the jurisdictions where the programs are targeted.

Nearly every federal law enforcement agency assisted in this effort by providing basic and advanced training courses in all aspects of financial criminal investigation. Likewise, bank regulatory agencies participated in providing advanced AML/CTF training to supervisory entities. In addition, INL made funds available for the intermittent or full-time posting of legal and financial mentors at selected overseas locations. These advisors work directly with host governments to assist in the creation, implementation, and enforcement of anti-money laundering and financial crime legislation. INL also provided several federal agencies funding to conduct multi-agency financial crime training assessments and develop specialized training in specific jurisdictions to combat money laundering.

The State Department, in conjunction with DHS' Immigration and Customs Enforcement (ICE) and the Department of Treasury, supports five trade transparency units (TTUs) in Latin America: three in the tri-border area of Brazil, Argentina, and Paraguay, one in Mexico, and one in Colombia. TTUs are entities designed to help identify significant disparities in import and export trade documentation and continue to enjoy success in combating money laundering and other trade-related financial crimes. The number of trade-based money laundering investigations emerging from TTU activity continues to grow. In 2008, Mexico's TTUs investigated seven cases; Colombia, four; Paraguay, six; and Argentina, two. Similar to the Egmont Group of FIUs that examines and exchanges information gathered through financial transparency reporting requirements, an international network of TTUs would foster the sharing of disparities in trade data between countries and be a potent weapon in combating customs fraud and trade-based money laundering. Trade is the common denominator in most of the world's alternative remittance systems and underground banking systems. Trade-based value transfer systems have also been used in terrorist finance.

The success of the Caribbean Anti-Money Laundering Program (CALP) convinced INL that a similar type of program for small Pacific island jurisdictions had the potential of developing viable AML/CTF regimes. Accordingly, INL funded the establishment of the Pacific Island Anti-Money Laundering Program (PALP) in 2005. The objectives of PALP are to reduce the laundering of the proceeds of all serious crime and the financing of terrorist financing by facilitating the prevention, investigation, and prosecution of money laundering. PALP's staff of resident mentors provides regional and bilateral AML/CTF mentoring, training and technical assistance to the 14 Pacific Islands Forum countries that are not members of the Financial Action Task Force (FATF). The management of the program was transferred to the UN Global Program against Money Laundering from the Pacific Islands Forum in September 2008, as the PALP began its third year of operation. INL will provide a total of nearly $6 million for the four-year PALP project.

Including the $1.5 million for the management of the PALP, INL obligated $2.2 million to the UN Global Program against Money Laundering (GPML) in 2008. In addition to sponsoring money laundering conferences and providing short-term training courses, GPML instituted a unique longer-term technical assistance initiative through its mentoring program. The mentoring program provides advisors on a year-long basis to specific countries or regions. GPML mentors provided assistance to the Secretariat of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) and to Horn of Africa countries targeted by the U.S. East Africa Counterterrorism Initiative. GPML resident mentors provided country-specific assistance to the Philippines FIU and asset forfeiture assistance to Namibia, Botswana, and Zambia. The resident mentor based in Namibia provided legal inputs to amend relevant legislation in each country, and initiated and monitored the Prosecutor Placement Program, an initiative aimed at placing prosecutors from the region for a certain period of time within the asset forfeiture unit of South Africa's national prosecuting authority. The GPML mentors in Central Asia and the Mekong Delta continued assisting the countries in those regions develop viable AML/CTF regimes. GPML continues to develop interactive computer-based programs, translated into several languages that are distributed to several regions globally.

INL continues to provide significant financial support for many of the anti-money laundering bodies around the globe. During 2008, INL supported FATF, the international AML/CTF standard setting

organization. In addition to sharing mandatory membership dues to FATF and the Asia Pacific Group on Money Laundering (APG) with the U.S. Department of the Treasury and DOJ, INL is a financial supporter of FATF-style regional bodies (FSRBs) secretariats and training programs, including the Council of Europe's MONEYVAL, the Caribbean Financial Action Task Force (CFATF), the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) and the South American Financial Action Task Force, Grupo de Accion Financiera de Sudamerica Contra el Lavado de Activos (GAFISUD). In 2008, INL also provided funding to the secretariat of the West African FSRB, Groupe Intergovernmental d'Action contre le Blanchiment d'Argent en Afriique de l'Ouest (GIABA), and has provided funding to GPML to place a residential mentor in Dakar, Senegal, to assist those member states of GIABA that have enacted the necessary legislation to develop FIUs. INL also financially supported the Organization of American States (OAS) Inter-American Drug Abuse Control Commission (CICAD) Experts Group to Control Money Laundering and the OAS Counter-Terrorism Committee. In preparation for the April 2009 Summit of the Americas, INL provided funding to CICAD and CICTE to persuade and assist those Latin American countries that have yet to criminalize the financing of terrorism to do so.

As in previous years, INL training programs continue to focus on both interagency bilateral and multilateral efforts. When possible, we seek participation with our partner countries' law enforcement, judicial and central bank authorities to design and provide training and technical assistance to countries with the political will to develop viable AML/CTF financing regimes. This allows for extensive synergistic dialogue and exchange of information. INL's approach has been used successfully in Africa, Asia, the Pacific, Central and South America, the Newly Independent States of the former Soviet Union, and Central Europe. INL also provides funding for many of the regional training and technical assistance programs offered by the various law enforcement agencies, including assistance to the International Law Enforcement Academies.

International Law Enforcement Academies (ILEAs)

The mission of the regional International Law Enforcement Academies (ILEAs) is to support emerging democracies, help protect U.S. interests through international cooperation, and promote social, political, and economic stability by combating crime. To achieve these goals, the ILEA program has provided high-quality training and technical assistance, supported institution building and enforcement capability, and fostered relationships between American law enforcement agencies with their counterparts in each region. ILEAs have also encouraged strong partnerships among regional countries to address common problems associated with criminal activity.

The ILEA concept and philosophy is the result of a united effort by all participants—government agencies and ministries, trainers, managers, and students—to achieve the common foreign policy goal of cohesive international law enforcement. This goal is to train professionals who will shape the future of the rule of law, human dignity, personal safety and global security.

The ILEAs are a progressive concept in the area of international assistance programs. Regional ILEAs offer three different types of programs. The core program, a series of specialized training courses, and regional seminars tailored to region-specific needs and emerging global threats. The core program typically includes 50 participants, normally from three or more countries. The specialized courses are comprised of about 30 participants and normally run one or two weeks long, often simultaneously with the core program. Lastly, there are regional seminars with different topics of interest, such as transnational crimes, financial crimes, and counterterrorism.

The ILEAs help to develop an extensive network of alumni who exchange information with their regional and U.S. counterparts and assist in transnational investigations. These graduates are also expected to be future leaders in their respective societies. The U.S. Department of State works with the U.S. Departments of Justice (DOJ), Homeland Security (DHS) and the Treasury, as well as with

foreign governments to implement the ILEA programs. To date, the combined ILEAs have trained more than 28,000 officials from more than 75 countries in Africa, Asia, Europe and Latin America.

Africa. ILEA Gaborone (Botswana) opened in 2001. Its main feature is a six-week intensive personal and professional development program, the Law Enforcement Executive Development Program (LEEDP), designed for mid-level law enforcement managers. The LEEDP brings together approximately 40 participants from several nations for instruction in areas such as combating transnational criminal activity, supporting democracy by stressing the rule of law in international and domestic police operations, and by raising the professionalism of officers involved in the fight against crime. ILEA Gaborone also offers specialized courses for police and other criminal justice officials to enhance their capacity to work with U.S. and regional counterparts to combat international criminal activities. These courses concentrate on specific methods and techniques in a variety of subjects, such as counterterrorism, anticorruption, financial crimes, border security, drug enforcement, firearms, and many others.

Instruction is provided to participants from Angola, Botswana, Lesotho, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Swaziland, Tanzania, Zambia, Djibouti, Ethiopia, Kenya, Uganda, Nigeria, Cameroon, Comoros, Congo, the Democratic Republic of Congo, Gabon, Madagascar, Burundi, Rwanda, Sierra Leone, Ghana, Guinea, and Senegal.

U.S. and Botswana trainers provide instruction. ILEA Gaborone has offered specialized courses on money laundering and terrorist financing-related topics such as criminal investigation, presented by the Federal Bureau of Investigation (FBI) and international banking and financial forensics, presented by DHS and DHS' Federal Law Enforcement Training Center (FLETC), and international money laundering schemes, presented by DHS' Immigration and Customs Enforcement (ICE). ILEA Gaborone trains approximately 500 students annually.

Asia. ILEA Bangkok (Thailand) opened in March 1999. This ILEA focuses on enhancing regional cooperation against the principal transnational crime threats in Southeast Asia: illicit drug trafficking, financial crimes, and alien smuggling. The ILEA provides a core course, the supervisory criminal investigator course (SCIC), designed to strengthen management and technical skills for supervisory criminal investigators and other criminal justice managers. In addition, it also presents one senior executive-level program and about 18 specialized courses, each lasting one to two weeks, in a variety of criminal justice topics. The principal objectives of the ILEA are the development of effective law enforcement cooperation within the member countries of the Association of Southeast Asian Nations (ASEAN), East Timor, and China (including Hong Kong and Macau), and the strengthening of each country's criminal justice institutions to increase its abilities to cooperate in the suppression of transnational crime.

Instruction is provided to participants from Brunei, Cambodia, East Timor, China, Hong Kong, Indonesia, Laos, Macau, Malaysia, Philippines, Singapore, Thailand, and Vietnam. Subject matter experts from the United States, Thailand, Japan, Netherlands, Philippines, and Hong Kong provide instruction. ILEA Bangkok has offered specialized courses on money laundering and terrorist financing-related topics such as computer crime investigations, presented by FBI and DHS, and complex financial investigations, presented by the Internal Revenue Service (IRS), FBI and, the Drug Enforcement Administration (DEA). ILEA Bangkok trains approximately 800 students annually.

Europe. ILEA Budapest (Hungary) opened in 1995. Its mission has been to support the region's emerging democracies by combating an increase in criminal activity that emerged against the backdrop of economic and political restructuring following the collapse of the Soviet Union. ILEA Budapest offers three different types of programs: an eight-week core course, regional seminars, and specialized courses in a variety of criminal justice topics. Instruction is provided to participants from Albania, Armenia, Azerbaijan, Bulgaria, Croatia, Georgia, Hungary, Kazakhstan, Kyrgyz Republic,

Macedonia, Moldova, Montenegro, Romania, Russia, Serbia, Slovakia, Slovenia, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan.

Trainers from 17 federal agencies and local jurisdictions from the United States, Hungary, Canada, Germany, United Kingdom, Netherlands, Ireland, Italy, Russia, Interpol, and the Council of Europe provide instruction. ILEA Budapest has offered specialized courses on money laundering and terrorist financing-related topics such as investigating and prosecuting organized crime and transnational money laundering, both presented by DOJ's Office of Overseas Prosecutorial Development, Assistance, and Training (OPDAT). ILEA Budapest trains approximately 800 students annually.

Global. ILEA Roswell (New Mexico) opened in September 2001. It offers a curriculum comprised of courses similar to those provided at a typical criminal justice university or college. These three-week courses have been designed and are taught by academics for foreign law enforcement officials. This ILEA is unique in its format and composition with a strictly academic focus and a worldwide student body. The participants are middle- to senior-level law enforcement and criminal justice officials from Eastern Europe, Russia, the states of the former Soviet Union, Association of Southeast Asian Nations (ASEAN) member countries, and the People's Republic of China (including the Special Autonomous Regions of Hong Kong and Macau), and member countries of the Southern African Development Community (SADC), plus other East and West African countries; the Caribbean, and Central and South American countries. The students are drawn from pools of ILEA graduates from the Academies in Bangkok, Budapest, Gaborone and San Salvador. ILEA Roswell trains approximately 350 students annually.

Latin America. ILEA San Salvador (El Salvador) opened in 2005. Its training program is similar to the ILEAs in Bangkok, Budapest and Gaborone. It offers a six-week Law Enforcement Management Development Program (LEMDP) for law enforcement and criminal justice officials as well as specialized courses for police, prosecutors, and judicial officials. In 2009, ILEA San Salvador will deliver four LEMDP sessions and approximately 20 specialized courses that will concentrate on attacking international terrorism, illegal trafficking in drugs, alien smuggling, terrorist financing, and financial crimes investigations. Segments of LEMDP focus on terrorist financing, presented by the FBI, and financial evidence and money laundering application, presented by FLETC and IRS. Instruction is provided to participants from: Antigua and Barbuda, Argentina, Barbados, Bahamas, Belize, Bolivia, Brazil, Chile, Colombia, Costa Rica, Dominica, Dominican Republic, Ecuador, El Salvador, Grenada, Guadeloupe, Guatemala, Guyana, Haiti, Honduras, Jamaica, Martinique, Mexico, Nicaragua, Panama, Paraguay, Peru, St. Kitts and Nevis, St. Vincent, St. Lucia, Suriname, Trinidad and Tobago, Uruguay, and Venezuela. ILEA San Salvador trains approximately 800 students per year

The ILEA Regional Training Center in Lima (Peru) opened in 2007 to complement the mission of ILEA San Salvador. The center augments the delivery of region-specific training for Latin America and concentrates on specialized courses on critical topics for countries in the southern cone and Andean regions. The RTC trains approximately 300 students per year.

Board of Governors of the Federal Reserve System (FRB)

An important component in the United States' efforts to combat and deter money laundering and terrorist financing is to verify that supervised organizations comply with the Bank Secrecy Act (BSA) and have programs in place to comply with the Office of Foreign Assets Control (OFAC) sanctions. In 2008, the FRB conducted training and provided technical assistance to bank supervisors and law enforcement officials in anti-money laundering (AML) and counterterrorist financing (CTF) tactics in partnership with regional supervisory groups or multilateral institutions, including the Middle East and North Africa (MENA) Financial Regulator's Training Initiative. The FRB also provided seminars in Anti-Money Laundering Examination and workshops in the Fundamentals of Fraud. Officials from Albania, Bahamas, Bolivia, Chile, Croatia, Czech Republic, Dominican Republic, Ecuador, Ghana,

Guatemala, Haiti, Honduras, Hong Kong, India, Indonesia, Israel, Japan, Korea, Lebanon, Mexico, Morocco, Nigeria, Panama, Paraguay. Peru, Philippines, Qatar, Russia, Turkey, Venezuela, and Zambia attended one or both of these events.

Due to the importance that the FRB places on international standards, the FRB's AML experts participate regularly in the U.S. delegation to the Financial Action Task Force (FATF) and the Basel Committee's AML/CTF expert group. The FRB is also an active participant in the U.S. Treasury Department's ongoing Private Sector Dialogue conferences, attending the Latin American session in Brazil and the Baltics meeting in Lithuania this year. Staff also meets frequently with industry groups and foreign supervisors to support industry best practices in this area.

The FRB presented training courses on 'International Money Movement' to domestic law enforcement agencies, including the Department of Homeland Security's Bureau for Immigration and Customs Enforcement (DHS/ICE), as well as at the Federal Law Enforcement Training Center (FLETC) during 2008.

Federal Bureau of Investigation (FBI), Department of Justice

During 2008, with the assistance of U.S. Department of State (DOS) funding, the U.S. Federal Bureau of Investigation (FBI) continued its extensive international training in combating terrorist financing, money laundering, financial fraud, and complex financial crimes, as well as training in conducting racketeering enterprise investigations. One such training program is the FBI's International Training and Assistance Unit (ITAU), located at the FBI Academy in Quantico, Virginia. ITAU coordinates with the Terrorist Financing and Operations Section (TFOS) of the FBI's Counterterrorism Division (CTD), as well as other divisions at FBI headquarters and in the field, to provide instructors for these international initiatives. FBI instructors, who are most often intelligence analysts, operational Special Agents (SAs) or Supervisory Special Agents (SSAs), rely on their experience to relate to the international law enforcement students as peers and partners in the training courses.

The FBI regularly conducts training through the International Law Enforcement Academies (ILEA) in Bangkok, Thailand; Budapest, Hungary; Gaborone, Botswana; and San Salvador, El Salvador. In 2008, the FBI delivered training in white collar crime investigations to 216 students from 16 countries at ILEA Budapest. At ILEA Bangkok, the FBI provided training to 60 students from Thailand in the Supervisory Criminal Investigators Course (SCIC). At ILEA Gaborone, the FBI provided antiterrorist financing training to 161 students from 22 African countries. At ILEA San Salvador, the FBI provided antiterrorist financing training to 120 students from El Salvador, Brazil, Paraguay, Peru, Uruguay, Colombia, Ecuador, Costa Rica, Guatemala, and Honduras.

In 2008, the FBI also conducted trainings, in conjunction with other U.S. agencies, for officials from Serbia, Macedonia, Morocco, Philippines, Paraguay, Algeria, Tanzania and Senegal. One such training involved FBI participation in an anti-money laundering conference in Serbia that the U.S. Department of Justice's Office of Overseas Prosecutorial Development (OPDAT) delivered to 100 students. Another involved FBI participation in an anti-money laundering workshop in Macedonia that OPDAT delivered to 35 students. Also in 2008, the FBI conducted, jointly with the Internal Revenue Service's (IRS) Criminal Investigative Division (CID), a one-week course on combating terrorist financing and money laundering for 181 international students from Morocco, Philippines, Paraguay, Algeria, Tanzania, and Senegal.

At the FBI Academy, the FBI included blocks of instruction on combating terrorist financing and/or money laundering for 18 students participating in Session #12 of the Latin American Law Enforcement Executive Development Seminar (LALEEDS); the students were from Colombia,

Ecuador, Paraguay, Argentina, Uruguay, Costa Rica, Nicaragua, Panama, Belize, El Salvador, Guatemala, Honduras, Chile, Bolivia, and the Dominican Republic. The FBI included similar blocks of instruction for 14 students participating in Session #3 of the Arabic Language Law Enforcement Executive Development Seminar (ALLEEDS); these students were from Djibouti, Egypt, Jordan, Morocco, Qatar, Sudan, the United Arab Emirates (UAE) and Yemen. As part of the FBI's Pacific Training Initiative's (PTI) Session #21, the FBI included terrorist financing instruction for 53 participants from 13 countries: Thailand, China, Australia, Hong Kong, Pakistan, Indonesia, Malaysia, Philippines, India, Korea, Singapore, Japan and the United States (Honolulu).

Federal Deposit Insurance Corporation (FDIC)

In 2008, the Federal Deposit Insurance Corporation (FDIC) continued to work in partnership with several federal agencies and international groups to combat money laundering and inhibit the flow of terrorist funding through training and outreach initiatives. In partnership with the U.S. Department of State, the FDIC hosted three anti-money laundering and counter financing of terrorism (AML/CTF) training sessions for 49 representatives from Jordan, Kuwait, Paraguay, Qatar, Saudi Arabia, Senegal, Thailand, and the West Africa Central Bank. The training sessions included discussions on the AML examination process, customer due diligence, and foreign correspondent banking risks and controls.

During the year, the FDIC also met with supervisory and law enforcement representatives from 15 countries to discuss AML issues, including examination policies and procedures, the USA PATRIOT Act, suspicious activity reporting requirements, and government information sharing mechanisms. Those countries included: Afghanistan, Chile, Ghana, Haiti, Japan, Laos, Madagascar, Malawi, Mongolia, Nigeria, Pakistan, Syria, Tanzania, Timor-Leste, and Ukraine.

Additionally, the FDIC traveled to Uruguay to provide AML/CTF training to approximately 40 regulators from the Banco Central del Uruguay. The session focused upon AML examination procedures and the AML risk assessment process expected of domestic depository institutions. Separately, an overview of the FDIC's role as a regulator and supervisor was presented to approximately 100 Uruguayan bankers and government officials.

To compliment the FDIC's strong AML/CTF training commitment, the FDIC participated in the second annual U.S.-Latin American Private Sector Dialogue in Miami, Florida. This U.S. Department of the Treasury initiative provides a forum for discussion among U.S. and Latin American banks about common issues related to money laundering and terrorist financing. The FDIC also participated in a seminar focusing on Islamic banking hosted by Perbadanan Insurans Deposit Malaysia (PIDM) in Kuala Lumpur, Malaysia.

The FDIC has eight full-time subject matter experts in the Washington, D.C., office dedicated to AML/CTF initiatives as well as a group of 28 individuals available to assist the U.S. Government (USG) with AML/CTF Financial System Assessments.

Financial Crimes Enforcement Network (FinCEN), Department of Treasury

The Financial Crimes Enforcement Network (FinCEN) is a bureau of the U.S. Department of the Treasury and is the U.S. financial intelligence unit (FIU). It participates and promotes international collaboration and information sharing to detect and deter illicit financial activities and helps other countries develop their FIUs, which is a valuable component of a country's anti-money laundering and counterterrorist financing (AML/CTF) regime. FinCEN coordinates and provides training and technical assistance to foreign nations seeking to improve their capabilities to combat money laundering, terrorist financing, and other financial crimes. FinCEN's international training program

has two primary focuses: (1) instruction and presentations to a broad range of government officials, financial regulators, law enforcement officers, and others on the subjects of money laundering, terrorist financing, financial crime, and on FinCEN's mission and operation; and (2) individualized training to FIU counterparts regarding FIU operations, analytical training via personnel exchanges and FIU development seminars. Much of FinCEN's work involves strengthening existing FIUs and the channels of communication used to share information to support anti-money laundering investigations. In support and assistance to other FIUs, FinCEN participates in personnel exchanges (from a foreign FIU to FinCEN and vice versa); supports delegation visits to foreign FIUs and other agencies from the intelligence, regulatory and law enforcement communities; and coordinates regional workshops.

In 2008, FinCEN hosted representatives from approximately 47 countries, including general orientations and consultations under the auspices of the U.S. Department of State's International Visitor Leadership Program, International Law Institute's Anti-Corruption Seminar, and the World Bank Program for Leadership in Financial Market Integrity. These visits, typically lasting one to three days, focused on topics such as money laundering trends and patterns, the Bank Secrecy Act, USA PATRIOT ACT, communications systems and databases, case processing, and the goals and mission of FinCEN. Representatives from foreign financial and law enforcement sectors generally spend one to two days at FinCEN learning about money laundering, the U.S. AML regime and reporting requirements, the national and international roles of an FIU, and various additional topics.

FinCEN gives assistance to new or developing FIUs that are not yet members of the Egmont Group of FIUs. The Egmont Group is comprised of FIUs that cooperatively agree to share financial intelligence and has become the standard-setting body for FIUs. FinCEN hosts FIU orientation visits and provides training and mentoring on FIU development. In 2008, FinCEN hosted representatives from Afghanistan, Tanzania, and Cameroon's nascent FIUs for orientation visits. These visits included an overview on various aspects of developing an FIU such as the legal framework in which the FIU operates, an FIU's international role and its cooperation with other FIUs, and an overview of Egmont Group request processing and information sharing.

For those FIUs that are fully operational, FinCEN's goals are to assist the unit in increasing effectiveness, improve the unit's information sharing capabilities, and expand the unit's understanding of money laundering and terrorist financing. As a member of the Egmont Group, FinCEN works closely with other member FIUs to provide training and technical assistance to countries and jurisdictions interested in establishing their own FIUs and obtaining candidacy for membership in the Egmont Group. FinCEN is currently sponsoring FIUs from ten jurisdictions for Egmont Group membership: Afghanistan, China, Jordan, Kuwait, Oman, Pakistan, Saudi Arabia, Suriname, Tanzania, and Yemen. Additionally, FinCEN works multilaterally through its representative on the Egmont Training Working Group to design, implement, and co-teach Egmont-sponsored regional training programs for Egmont Group members as well as Egmont candidate FIUs.

In addition to hosting delegations for training on FinCEN premises, FinCEN conducts training courses and seminars abroad, both independently and in conjunction with other domestic and foreign agencies, counterpart FIUs, and international organizations. Occasionally, FinCEN's training and technical assistance programming is developed jointly with these other agencies to address specific needs of the jurisdiction or country receiving assistance. Such trainings provide trainees with improved knowledge and understanding of topics related to money laundering and terrorist financing, which include topics such as: FIU primary and secondary functions, regulatory issues, international case processing procedures, technology infrastructure and security, and terrorist financing and money laundering trends and typologies. In 2008, FinCEN conducted training seminars in Nigeria, Kuwait, Kazakhstan, Uzbekistan, and Afghanistan. The training focused on enhancing the capacity and cooperation of FIUs to combat money laundering and the financing of terrorism.

FinCEN conducts core analytical training to counterpart FIUs, both at FinCEN and abroad, and often in conjunction with other U.S. agencies. FinCEN's analytical training program, typically delivered over the course of one to two weeks, provides foreign analysts with basic skills in critical thinking and analysis; data collection; database research; suspicious transactions analysis; the intelligence cycle; charting; data mining; and case presentation. In 2008, FinCEN collaborated with Mexico's FIU and provided training on basic analytical skills to FIUs from Mexico, Belize, Guatemala, El Salvador, Panama, Honduras, and Colombia. Over the past twelve months, in an effort to reinforce the sharing of information among established Egmont member FIUs, FinCEN conducted personnel exchanges with Egmont Group members from Latvia, Mexico, South Africa, Australia, Netherlands, the United Kingdom, Canada, and Korea. These exchanges offer the opportunity for FIU personnel to see first-hand how other FIUs operates; to develop joint analytical projects and other strategic initiatives; and also to work jointly on on-going financial crimes cases. The participants in these exchanges share ideas, innovations, and insights that lead to improvements in such areas as analysis, information flow, and information security at their home FIUs, in addition to deeper and more sustained operational collaboration.

Immigration and Customs Enforcement, Department of Homeland Security (DHS)

During 2008, the U.S. Department of Homeland Security's (DHS) Immigration and Customs Enforcement (ICE), Financial, Narcotics and Public Safety Division, in conjunction with the DHS Office of International Affairs, delivered training to law enforcement, regulatory, banking, and trade officials from more than 60 countries to combat money laundering, terrorist financing, and bulk cash smuggling, and to conduct financial investigations. The training was conducted in both bilateral and multilateral engagements. ICE money laundering and financial investigations training is based on the broad experience and expertise achieved by leading U.S. efforts in investigating international money laundering and financial crimes as part of the former U.S. Customs Service.

Bulk Cash Smuggling

Using primarily U.S. Department of State funding, ICE provided bilateral and multilateral training and technical assistance on the interdiction and investigation of bulk cash smuggling (BCS) for 390 officials from 30countries. Notably, ICE conducted two BCS training conferences in Iraq for more than 65 Iraqi security and police forces. ICE also provided basic BCS training in the Argentina, Malaysia, Indonesia, Thailand, Egypt, Nigeria, Mauritania, and Georgia.

ICE, with the participation of Australian officials, conducted a regional training program for three countries that had completed the basic and advanced BCS modules BCS: the Philippines, Malaysia, and Indonesia. This week-long regional program was intended to encourage participating countries to share information with counterpart agencies in neighboring countries. Thailand, which has received only the basic BCS course, participated in the training as an observer. ICE also conducted BCS training in Amman, Jordan, to officials from 11 member states of the Middle East and North Africa Financial Action Task Force (MENA-FATF), including Lebanon, Egypt, Kuwait, Yemen, Oman, Algeria, Qatar, Mauritania, Morocco, Tunisia, and Jordan. Officials from the Palestinian Authority also attended this conference.

Through the U.S. Department of State's International Law Enforcement Academy (ILEA) programs, ICE conducted in 2008 more than 50 financial investigations and anti-money laundering training programs for more than 755 participants. The participants represented law enforcement personnel from 69 countries.

Trade Transparency Units (TTUs)

Trade Transparency Units (TTUs) identify anomalies related to cross-border trade that are indicative of international trade-based money laundering. TTUs generate, initiate, and support investigations and prosecutions related to trade-based money laundering, the illegal movement of criminal proceeds across international borders, alternative money remittance systems, and other financial crimes. By sharing trade data, ICE and participating foreign governments are able to see both sides of import and export transactions for commodities entering or exiting their countries, thus assisting in the investigation of international money laundering organizations

With funding from the U.S. Department of State's Bureau of International Narcotics and Law Enforcement (INL), ICE worked to expand the network of operational TTUs beyond Colombia, Brazil, Argentina, and Paraguay by providing IT equipment and training to the newly established TTU in Mexico City, Mexico. As Mexico is a major trading partner with the United States, the Mexico unit is the largest TTU initiative to date.

In 2008, ICE updated the technical capabilities of existing TTUs and trained new TTU personnel in Colombia, Paraguay, and Mexico as well as members of their financial intelligence units. Additionally, ICE strengthened its relationship with its TTUs by deploying temporary and permanent personnel overseas to work onsite and provide hands on training to all five TTUs in the hemisphere. This action has continued to facilitate the information sharing between the U.S. Government and foreign TTUs in furtherance of ongoing joint criminal investigations.

Other ICE Programs

Additionally in 2008, ICE expanded Operation Firewall, a joint strategic bulk cash smuggling initiative with DHS' U.S. Customs and Border Protection (CBP) to provide hands-on training and capacity building to law enforcement officials in Mexico, Honduras, El Salvador, Guatemala, Panama, Colombia, Ecuador, and Dominican Republic. Operation Firewall was initiated to address the threat posed by bulk cash smuggling via all modes of transportation at air and land ports of entry. In fiscal year (FY) 2008, Operation Firewall resulted in approximately 978 seizures totaling more than $51 million in U.S. currency and negotiable instruments.

Under the ICE Cornerstone initiative, training was developed and designed to provide the financial and trade sectors with the necessary skills to identify and develop methodologies to detect suspicious transactions indicative of money laundering and criminal activity. In furtherance of Cornerstone, ICE has appointed field and headquarters agents who are dedicated to providing training to the financial and trade communities on identifying and preventing exploitation by criminal and terrorist organizations. In FY 2008, ICE Cornerstone liaisons conducted 884 outreach meetings with more than 21,000 industry professionals in the U.S. and abroad.

Internal Revenue Service (IRS), Criminal Investigative Division (CID) Department of Treasury

In 2008, the U.S. Internal Revenue Service (IRS) Criminal Investigative Division (CID) continued their involvement in international training and technical assistance efforts designed to assist international law enforcement officers in detecting tax, money laundering, and terrorist financing crimes. With funding provided by the U.S. Department of State, IRS-CID delivered training through agency and multi-agency technical assistance programs to international law enforcement agencies. Training consisted of both basic and advanced financial investigative techniques.

IRS-CID participated in delivering State Department-funded courses to combat terrorism financing and money laundering, which were hosted by the Federal Bureau of Investigation (FBI) in Morocco, Paraguay, Algeria, Tanzania, and Senegal. IRS-CID conducted a financial investigative technical course in Asuncion, Paraguay, funded by an interagency agreement between the U.S. Department of State's Bureau for International Narcotics and Law Enforcement Affairs (INL) and the U.S. Department of the Treasury's Office of Technical Assistance (OTA). The training program was attended by 40 officials from the government of Paraguay, including the Ministry of Finance's Tax Department, the Customs Office, the Prosecutors' Office, the Secretary for the Prevention of Money Laundering, the Justice Department, and the Trademark Office. IRS-CID also conducted financial investigative techniques classes in Tirana and Durrës, Albania. The focus of the courses was money laundering relating to public corruption and the target audience was the newly formed Joint Investigative Unit for Economic Crimes and Corruption (JIU). The classes were comprised of both prosecutors and investigators from the JIU and also included non-JIU participants. Investigators and prosecutors from Albania's many provincial areas were represented in the class.

IRS-CID provided instructor and course delivery support to the four International Law Enforcement Academies (ILEAs) run by the State Department in Bangkok, Thailand; Budapest, Hungary; Gaborone, Botswana; and San Salvador, El Salvador. At ILEA Bangkok, IRS-CID participated in one supervisory criminal investigator course and was the coordinating agency of the complex financial investigations course. These courses were provided to senior, mid-level, and first-line law enforcement supervisors and officers from Brunei, Cambodia, Hong Kong, Indonesia, Laos, Macau, Malaysia, Maldives, Philippines, Singapore, Thailand, Timor-Leste, and Vietnam. Also at ILEA Bangkok, IRS-CID conducted a complex financial investigations course sponsored by OPDAT. Various Thai government agencies attended this course, including the police, and officials involved in anti-money laundering, customs enforcement, consumer protection, counternarcotics, insurance regulation, and securities and exchange regulation.

At ILEA Budapest, IRS-CID participated in five sessions delivering financial investigative techniques training. IRS-CID also provided a class coordinator for a six-week ILEA course, the Core Program Session #65, for which the IRS-CID coordinator held the responsibility of coordinating and supervising the participant's daily duties and activities. The countries that participated in these classes were Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Georgia, Hungary, Kazakhstan, Macedonia, Moldova, Romania, Russia, Serbia, and Ukraine. At ILEA Gaborone, IRS-CID participated in four Law Enforcement Executive Development programs, delivering financial investigative techniques training. Countries that participated in these classes were Angola, Botswana, Lesotho, Malawi, Mauritius, Mozambique, Namibia, South Africa, Swaziland, Tanzania, Zambia, Djibouti, Ethiopia, Kenya, Seychelles, Uganda, Nigeria, Cameroon, Comoros, the Republic of the Congo, Gabon, and Madagascar. At ILEA San Salvador, IRS-CID participated in three of the Law Enforcement Management Development Programs (LEMDP), delivering financial investigative techniques training. Countries that participated in these classes were Antigua and Barbuda, Argentina, Bahamas, Barbados, Belize, Chile, El Salvador, Grenada, Guatemala, Jamaica, Mexico, Paraguay, Peru, St. Kitts and Nevis, and Suriname. LEMDP stresses the importance of conducting a financial investigation to further develop a large scale, criminal investigation.

Office of the Comptroller of the Currency (OCC), Department of Treasury

The U.S. Department of the Treasury's Office of the Comptroller of the Currency (OCC) performs on-site examinations and provides Bank Secrecy Act (BSA) and anti-money laundering (AML) guidance to national banks and federal branches of foreign banking organizations. On-site examinations include reviewing compliance with BSA/AML laws and regulations at some of the largest financial

institutions in the world. Working with other federal banking regulators through the Federal Financial Institution Examination Council (FFIEC), the OCC assists with developing and providing BSA/AML guidance and training to examiners and foreign banking supervisors. Such initiatives include maintaining the FFIEC BSA/AML examination manual, providing instructors for FFIEC AML compliance workshops, and providing speakers for the FFIEC advanced BSA/AML compliance conference.

The OCC conducted and sponsored a number of anti-money laundering initiatives for foreign banking supervisors during 2008. In June, the OCC sponsored its Anti-Money Laundering and Counter Financing of Terrorism (AML/CTF) School in Washington, D.C. The school was designed specifically for foreign banking supervisors to increase their knowledge of money laundering and terrorist financing activities and how these acts are perpetrated. The course provided a basic overview of AML examination techniques, tools, and case studies. Banking supervisors from 19 countries attended the school at the OCC's Washington, D.C., headquarters, including Algeria, Argentina, Austria, Belize, India, Italy, Korea, Mexico, Netherlands, Nigeria, Panama, Philippines, St. Vincent and the Grenadines, and Turkey. The OCC also contributed personnel to a Middle East Northern Africa Regional AML Seminar in Casablanca, Morocco, during July that assisted government personnel from Morocco, Egypt, Lebanon, and Qatar. AML technical assistance was also provided to banking supervisors from Uruguay and Russia through participation on AML/CTF on-site examinations. Various OCC officials participated in international conferences on combating money laundering. In March and May of 2008, OCC officials were part of a body of U.S. regulators that presented at the Money Laundering Alert's International Conference on Combating Money Laundering and the Institute of International Bankers 2008 Annual Anti-Money Laundering Seminar.

Office of Overseas Prosecutorial Development, Assistance and Training, the Asset Forfeiture and Money Laundering Section, & Counterterrorism Section (OPDAT, AFMLS, and CTS), Department of Justice

Training and Technical Assistance

The U.S. Department of Justice's (DOJ) Office of Overseas Prosecutorial Development, Assistance, and Training (OPDAT) assesses, designs, and implements training and technical assistance programs for U.S. criminal justice sector counterparts overseas. OPDAT draws upon the anti-money laundering and counter financing of terrorism (AML/CTF) expertise within DOJ, including the Asset Forfeiture and Money Laundering Section (AFMLS), Counterterrorism Section (CTS), and U.S. Attorney's Offices, to train and advise foreign AML/CTF partners. Much of the assistance provided by OPDAT and AFMLS is provided with funding from the U.S. Department of State.

In addition to training programs targeted to a country's immediate needs, OPDAT also provides long-term, in-country assistance through Resident Legal Advisors (RLAs). RLAs are federal prosecutors who provide in-country technical assistance to improve capacity, efficiency, and professionalism within foreign criminal justice systems. RLAs are posted to U.S. Embassies for a period of one or two years to work directly with counterparts in legal and law enforcement agencies, including ministries of justice, prosecutor's offices, and offices within the judiciary branch. To promote reforms within the criminal justice sector, RLAs provide assistance in legislative drafting, modernizing institutional structures, policies and practices, and training law enforcement personnel, including prosecutors, judges, police, and other investigative or court officials. For all programs, OPDAT draws upon

expertise from DOJ's Criminal Division, the National Security Division, AFMLS, and other DOJ components as needed.

Money Laundering/Asset Forfeiture/Fraud

In 2008, OPDAT and AFMLS provided training to foreign judges, prosecutors, and other law enforcement officials, and provided assistance in drafting anti-money laundering statutes compliant with international standards. Such assistance enhanced the ability of participating countries to prevent, detect, investigate, and prosecute money laundering, and to make appropriate and effective use of asset forfeiture. The content of individual technical assistance programs varied, depending on the participants' specific needs, but topics addressed in 2008 included money laundering legislation development, international AML/CTF standards compliance, techniques and methods used for effective investigations, and prosecution of money laundering, including the role of prosecutors, criminal and civil forfeiture systems, and the importance of both international and inter-agency cooperation and communication.

AFMLS provides direct technical assistance in connection with legislative drafting on all matters involving money laundering, asset forfeiture, and the financing of terrorism. In 2008, AFMLS provided such assistance to nine countries, including Azerbaijan, Haiti, India, Indonesia, Kosovo, Kyrgyz Republic, Liberia, Turkey, and Vietnam. AFMLS provided training on money laundering issues in Albania, Armenia, Bangladesh, Bosnia, China, Colombia, Croatia, Georgia, Hungary, Kazakhstan, Kyrgyz Republic, Macedonia, Moldova, Montenegro, New Zealand, Serbia, Turkey, Ukraine, and Uzbekistan. In addition, AFMLS continued to participate in meetings of the Organization of American States (OAS) Inter-American Drug Abuse Control Commission (CICAD) Experts Group on Money Laundering to develop and promote best practices in money laundering and asset forfeiture. AFMLS also participated in the Camden Asset Recovery Inter-Agency Network (CARIN) Group on asset recovery.

In an effort to improve international cooperation, AFMLS, in conjunction with Poland's ministry of justice, co-hosted a conference in April in Krakow, Poland, on international forfeiture cooperation among prosecutors and investigators. This conference brought practitioners, investigators, and international experts together to discuss experiences and provide practical tools to further international forfeiture cooperation. Officials from Bulgaria, Estonia, Latvia, Liechtenstein, Moldova, Poland, Romania, Switzerland, Ukraine, and the United States participated.

In April 2008, AFMLS conducted a conference on international issues in asset forfeiture that covered international asset sharing, obtaining evidence and assistance from foreign countries, black market peso exchanges, terrorist financing, and digital currency and e-gold investigations. More than 30 foreign prosecutors attended from Brazil, Canada, Georgia, Guernsey, Switzerland, Thailand, and the United Kingdom.

In October 2008, AFMLS developed an international conference that focused on AML/CTF and corruption issues. The conference was held in Budapest, Hungary, and was attended by the Prosecutors General and deputies of Albania, Armenia, Bosnia, China, Croatia, Georgia, Hungary, Kazakhstan, Kyrgyz Republic, Macedonia, Moldova, Montenegro, Serbia, Turkey, Ukraine, and Uzbekistan.

With U.S. Department of State funding, OPDAT provided training to government officials on money laundering and financial crime-related issues to officials from more than 20 countries, including Albania, Armenia, Azerbaijan, Bangladesh, Bosnia and Herzegovina, Brazil, Bulgaria, Georgia, Grenada, Indonesia, Jordan, Kosovo, Kuwait, Liberia, Macedonia, Paraguay, Russia, Serbia, Trinidad and Tobago, Ukraine, and the United Arab Emirates.

Training for Local Judiciary and Investigators in Serbia. OPDAT provided a series of trainings to enhance local judiciary and law enforcement capacity to investigate, prosecute, and adjudicate money laundering and terrorism financing cases. The objectives of these trainings were to build Serbian prosecutor and investigator capacity to conduct complex financial investigations, and to promote cooperation among prosecutors and investigators, as well as with different institutions providing assistance on financial matters.

New Money Laundering Law for Albania. OPDAT participated in a working group tasked with drafting a new AML/CTF law in Albania. In May 2008, the new law passed, lowering the reporting threshold for financial transactions and enhancing customer identification requirements.

Assistance to the Bangladesh FIU. OPDAT provides to the Bangladesh Financial Intelligence Unit (FIU) regular assistance to enable it to become the first South Asian nation admitted to the Egmont Group. To that end, OPDAT has sponsored several FIU advisors to work directly with the central bank of Bangladesh. In 2008, OPDAT sponsored two such advisors for three-week assignments each.

Money Laundering/Asset Forfeiture Training in Brazil. In 2008, OPDAT's RLA to Brazil formed a working group that includes a federal money laundering judge, prosecutors, and law enforcement officials. This group meets regularly and plans to draft an "undercover manual" for money laundering investigations. In addition, the RLA is planning a national money laundering course for Brazil's 27 federal money laundering judges, the prosecutors who work in their courts, and law enforcement personnel.

Money Laundering/Asset Forfeiture Program in Azerbaijan. OPDAT's RLA to Azerbaijan held a one-day seminar for members of Parliament, the Ministry of Justice, nongovernmental organizations, and the press, to discuss pending draft legislation on the money laundering law. At the seminar, the 60 participants vigorously debated and ultimately voiced their support for the passage of a Financial Action Task Force (FATF) complaint money laundering law. This draft law recently passed in second reading in Azerbaijan's parliament.

AML Training for Russian Police and Prosecutors. OPDAT's RLA to Russia works on an ongoing basis with the Russian FIU, the FSFM, to plan training on AML and terrorism financing prevention and detection for the ministry of internal affairs. The RLA facilitates communication between DOJ's Organized Crime and Racketeering Section and the FSFM on money laundering cases, works closely with the Department of the Treasury's Office of Technical Assistance (OTA) representative to the FSFM on training and case cooperation issues, and represents DOJ at U.S. Embassy Moscow's anti-money laundering working group.

Financial Crimes Trainings in Ukraine. In 2008, OPDAT conducted several half-day training modules on the investigation of complex financial crimes and money laundering. Between May and December, OPDAT conducted five of these training modules at the Ukraine Academy of Prosecutors for a total of 300 prosecutors enrolled in continuing education courses. In October, OPDAT conducted two of these training modules for the 250 future prosecutors enrolled in the master's degree program at the Academy of Prosecutors. In November, OPDAT conducted three of these training modules for 200 undergraduate law students enrolled at the specialized Ministry of Interior University, the State Security Service Academy, and the National Law Academy in Lviv.

Asset Forfeiture Legislation and Workshops in Ukraine. Between May and September, OPDAT, in cooperation with AFMLS, worked with Ukraine's ministry of justice on the drafting of a new law on asset forfeiture. That draft has since been forwarded to the cabinet of ministers for consideration. In 2008, OPDAT also presented a speech on asset forfeiture at an international roundtable that included representatives of Ukraine's ministry of justice, prosecutor general's office, and the academy of prosecutors.

Support for AML Reform and Specialization in Ukraine. OPDAT worked with Ukraine's FIU and with the cabinet of ministers to improve Ukraine's AML regime, and to develop an annual AML action plan, issued by the cabinet of ministers, which specifically calls for greater specialization of AML prosecutors and investigators. OPDAT participated in two international AML conferences, in April and June, speaking to approximately 70 lawyers and investigators from Ukraine's procuracy, its FIU, and the ministry of justice. OPDAT also supported the participation of several Ukrainian prosecutors at those conferences.

AML Assistance to Georgia. In 2008, with OPDAT's facilitation, U.S. agents from the U.S. Federal Bureau of Investigation (FBI) polygraphed members of Georgia's new Anti-Money Laundering Unit (AMLU). The polygraphs protect the office of public prosecutions (OPP) from charges that they replaced a polygraphed unit with a nonpolygraphed unit. After completing the polygraphs, an OPDAT and a U.S. Department of the Treasury advisor conducted two seminars to improve the OPP's ability to combat money laundering. In the first seminar, OPP, Georgia's financial monitoring service (FMS), and the ministry of internal affairs (MOIA) investigative unit participated in a roundtable to improve communications between the various units.

AML Seminars in Georgia. OPDAT and the U.S. Department of the Treasury coordinated a series of seminars with the aim of increasing communications among the AMLU, FMS, and MOIA. One such roundtable sought to teach the three agencies to work as a single unit to prosecute money laundering cases. The roundtable prepared the agencies for an anti-money laundering seminar at which U.S. money laundering experts assisted the three agencies with improving and increasing their anti-money laundering prosecutions. OPDAT also sponsored a second seminar to discuss money laundering issues with representatives from the AMLU, FMS, and MOIA, as well as Armenian prosecutors and financial investigators.

Asset Forfeiture Assessment in Albania. In May, OPDAT brought two members of the Asset Forfeiture Division of the U.S. Marshals Service to Albania to conduct a preliminary assessment of the country's asset forfeiture laws and administration. The assessment provided an excellent opportunity to highlight areas in need of improvement and plans for specialized asset forfeiture training. The visit also helped prompt some action by the Albanian government to physically secure seized terrorism-related assets.

Asset Forfeiture Legislation in Indonesia. OPDAT's RLA to Indonesia has worked with an Indonesia interagency team to draft Indonesia's first asset forfeiture law. In July, OPDAT organized a drafting workshop with the draft team and an AFMLS asset forfeiture expert. In addition to providing an overview of various countries' asset forfeiture, asset sharing, and asset management regimes, the AFMLS expert provided for discussion by the team a section-by-section analysis of each of the 44 provisions in the draft Indonesia law.

Financial Crimes Program in Grenada. In January, OPDAT conducted the second phase of a financial crimes program in the St. George's section of Grenada for approximately 20 prosecutors and law enforcement officials. During the prior phase in 2007, participants had developed a handbook, for both operational and training purposes, that standardized the processes involved in investigating and prosecuting financial crimes in Grenada. During this second phase, the emphasis was on practical exercises, such as conducting searches for financial records.

AML Program in Bangladesh. In January, OPDAT, AFMLS, and FBI conducted an anti-money laundering program in Dhaka. The program was twofold—to provide technical advice to the Bangladesh Corruption Task Force on cases that have monetary links to the United States and to meet with officials from the law ministry, attorney general's office, and the Bank of Bangladesh about AML/CTF legislation that could help Bangladesh's FIU to qualify for admission to the Egmont Group.

Police/Investigators/Prosecutors Training in Serbia. In February, OPDAT's RLA to Serbia, in conjunction with the American Bar Association Central Europe and Eurasia Law Initiative and the Organization for Security and Cooperation in Europe (OSCE), conducted programs for prosecutors, police, and other investigators on combating financial crimes, in Pancevo and Belgrade, Serbia.

FIU Assistance in Kuwait. OPDAT's RLA to the United Arab Emirates, in conjunction with AFMLS, OTA, and the Financial Crimes Enforcement Network (FinCEN), organized an FIU implementation program in Kuwait City, Kuwait. The U.S. Government (USG) representatives met with Kuwaiti officials to assist them in developing a blueprint to improve the effectiveness of their FIU and make it eligible for admission to the Egmont Group.

Money Laundering and Asset Forfeiture Workshops in Macedonia. In February, OPDAT's RLA to Macedonia conducted two workshops in Skopje, Macedonia on investigating and prosecuting money laundering and asset forfeiture cases. The objective of these two workshops, which were presented to prosecutor and judge candidates at the National Training Academy, was to familiarize them with basic good practices and lessons learned in prosecuting money laundering offenses domestically and internationally.

Training on Financial Crimes Investigation and Prosecution Bosnia and Herzegovina. In March, OPDAT conducted training on investigation and prosecution of financial crimes for prosecutors as well as tax and police inspectors. Emphasis was placed on asset forfeiture and police-prosecutor cooperation.

Asset Seizure Legislation in Serbia. From March to June, OPDAT's RLA to Serbia, in cooperation with the OSCE, participated in meetings of the Serbian asset seizure working group, and supported two working group retreats, at which the group finalized the asset seizure bill. This is the culmination of DOJ assistance to the working group, which has included programs on international best practices, examinations of asset forfeiture regimes from other countries, and a detailed review of the Serbian draft law on asset seizure. The Parliament adopted its first ever asset seizure law in October 2008.

Financial Crimes Workshop in Trinidad & Tobago. OPDAT, in partnership with OTA and the U.S. Embassy in Port-of-Spain, Trinidad & Tobago, conducted a workshop on combating financial crimes for approximately 25 representatives from the Government of Trinidad and private industry. The purpose was to enhance the ability of Trinidad's prosecutors and investigators to investigate and prosecute financial crimes; to that end, the participants drafted a handbook of best practices for investigating and prosecuting financial crimes.

Financial Crimes Workshop in Bulgaria. In May, OPDAT and DOJ's Organized Crime and Racketeering Section, in conjunction with Bulgaria's prosecutorial training facility, the National Institute of Justice (NIJ), conducted a financial crimes workshop in Sofia for 35 Bulgarian prosecutors who specialize in money laundering and other financial crimes. The workshop covered money laundering investigations and prosecutions in the United States and how they compare to Bulgarian cases. The program will be adopted into the permanent curriculum of the NIJ.

U.S. Study Tour on AML Issues for a Delegation from Bangladesh. In July, OPDAT organized a week-long, U.S.-based study tour for Bangladesh's Home Secretary and the Deputy Governor of the Bank of Bangladesh. The delegation learned about avenues of international cooperation and the ramifications of a positive or negative AML/CTF assessment by the Asia Pacific Group FATF-style regional body.

Intellectual Property and Financial Crimes Programs in Trinidad & Tobago. In September, OPDAT conducted two workshops in Port-of-Spain, Trinidad & Tobago, one to enhance the ability of Trinidad law enforcement officials to combat intellectual property rights (IPR) crimes, and the other to assist them in fighting financial crimes. The IPR program included practical exercises, such as conducting searches. The financial crimes program focused on developing strategies for combating financial and

financially-motivated crimes, as well as enhancing collaboration with the financial sector. Participants to both workshops included police, prosecutors, and representatives of the financial sector.

Financial Investigative Techniques Training in Paraguay. In September, OPDAT, jointly with OTA and the Internal Revenue Service's Criminal Investigative Division (IRS-CID), coordinated a week-long advanced money laundering course for 42 Paraguayans, including prosecutors from the financial crimes and anticorruption unit, judges, FIU investigators, and analysts from the tax and customs investigative units. The course focused on money laundering investigative techniques and instructors taught participants to analyze bank accounts and financial documents in several hypothetical money laundering cases.

Task Force Development Program in Jordan. In October, OPDAT, in collaboration with OTA, conducted a seminar in Amman, Jordan, on task force development for Jordanian prosecutors, investigators, and judges. The program focused on using the task force approach in the investigation and prosecution of organized crime. The agenda covered definitions and examples of international organized crime; enterprise theory of investigating and prosecuting organized crime; money laundering, racketeering, gang, and corruption offenses; specialized forensics and investigative techniques; and organizing a case involving complex financial crimes, including terrorism financing.

Financial Crimes Seminar in Liberia. In October, OPDAT's RLA to Liberia conducted a financial crimes seminar in Monrovia, Liberia, for 50 Liberian criminal prosecutors and investigators. The primary objectives were to introduce the concept of long term investigations; encourage a working relationship between criminal investigators and prosecutors; present better practices in the areas of ethics and organization; and show how basic financial crimes investigative techniques can be used in corruption cases.

Suspicious Transaction Reporting Seminar in Armenia. In November, OPDAT, in coordination with the U.S. Department of State's Bureau of International Narcotics and Law Enforcement (INL) and FinCEN, held a three-day training program on the generation and analysis of suspicious transaction reports. Thirty Armenian bankers, financial investigators, and prosecutors attended the seminar; the topics included various analytic tools such as data mining, the use of link analysis, and prioritizing suspicious targets.

Embedded Prosecutor within Bulgarian Prosecution Service. A prosecutor from DOJ's Organized Crime and Racketeering Section began in 2008 to mentor Bulgarian prosecutors working on some of the country's most sensitive organized crime and corruption cases, with special focus on two key money laundering cases. The prosecutor also provides advice to a U.S. Embassy team that is working with the Bulgarian Prosecution Service and Ministry of Interior to develop an organized crime task force that would target some of the country's most elusive organized crime figures.

Tracing Illegal Proceeds in Brazil. OPDAT's RLA to Brazil, in conjunction with FBI, developed a course on tracing illegal money used for criminal conduct. The course was held in August 2008 in Rio de Janeiro and more than 200 participants attended, including law enforcement, judges, and prosecutors.

Crimes Against the Credit System, Against Creditors, Fraud and Embezzlement. In July, OPDAT held a seminar for 25 Bulgarian prosecutors on crimes against the credit system, crimes against creditors, and fraud and embezzlement. This course will be adopted into the permanent curriculum of Bulgaria's National Institute of Justice, the country's official training institution for judges and prosecutors.

Financial Investigative Techniques Training to Combat Corruption in Albania. In April, OPDAT's two RLAs to Albania, assisted by three IRS criminal investigative experts, conducted two week-long intensive seminars on effective financial investigative techniques for prosecutors and investigators. The trainings concentrated on practical exercises involving cases of money laundering, asset forfeiture, and public corruption. These seminars are part of a series of specialized training sessions,

begun in December 2007, designed to increase the capacity of the newly-created Joint Investigative Unit to fight economic crime and corruption in the Tirana district prosecution office.

Third South Africa Judicial Colloquium on Racketeering and Asset Forfeiture. In May, OPDAT coordinated a three-day colloquium for South African judges on the subject of racketeering in Cape Town. The colloquium focused on racketeering, the use of crime participants as witnesses, and the use of asset forfeiture in combating criminal organizations. The colloquium was the third in an on-going series of such programs.

U.S. Study Tour for Macedonian Prosecutors. In May, OPDAT's RLA to Macedonia hosted a nine-person delegation from Macedonia to visits to Madison, Wisconsin, and New York, New York. The delegation included prosecutors who specialized in organized crime and financial crimes. The focus of the study tour was to examine the prosecution of money laundering cases and the use of task force building.

Organized Crime and Fraud Training in China. In calendar year 2008, OPDAT's RLA to China lectured on investigative techniques in organized crime prosecutions to ten different audiences throughout China, including prosecutors, judges, and law students. In September, the RLA facilitated a presentation by DOJ's Fraud Section on best practices from the Katrina Fraud Task Force to the Chinese ministry of supervision and others in the Chinese government responsible for monitoring fraud in the use of relief funds for the Sichuan province earthquake.

Assistance in Combating Organized Crime in Serbia. In February, OPDAT's RLA to Serbia, in conjunction with the UN Office on Drugs and Crime, conducted training for Serbia's organized crime prosecutor's office on analyst notebook software, which OPDAT donated to the prosecutor's office. The office handles a high volume of complex corruption and economic crimes cases, including money laundering during the Milosevic era, judicial bribery cases, fraud and corruption of Serbian government officials, and international smuggling cases. The software, related equipment, and training will permit the organized crime units of prosecutors and police to work more effectively together in analyzing, organizing, and later presenting evidence in court.

U.S.-Bulgaria Mutual Legal Assistance and Extradition Treaties. In June, OPDAT organized with the Bulgarian Association of Prosecutors a two-and-a-half day training for 30 prosecutors and five officials from the ministry of justice on the new Mutual Legal Assistance Agreement and Extradition Treaties between the two countries. Presenters came from DOJ's Office of International Assistance, the State Department's Office of the Legal Advisor, and the International Department of the Bulgarian Supreme Cassation Prosecution Service.

Asset Management System Assessment in Macedonia. OPDAT, with the assistance of the U.S. Marshals Service, conducted an assessment of Macedonia's current seized and forfeited assets management system. In a specialized workshop, OPDAT and the U.S. Marshals Service presented to the Macedonian government a set of recommendations for the government to consider on how to create an efficient and corruption-free assets management system.

Terrorism/Terrorist Financing

OPDAT, CTS, and AFMLS, with the assistance of other DOJ components, play a central role in providing technical assistance to foreign counterparts, both to attack the financial underpinnings of terrorism and to build legal infrastructures to combat it. In this effort, OPDAT, CTS, and AFMLS work as integral parts of the interagency U.S. Terrorist Financing Working Group (TFWG), co-chaired by the State Department's INL bureau and the Office of the Coordinator for Counterterrorism (S/CT).

The TFWG supports seven RLAs assigned overseas, located in Bangladesh, Indonesia, Kenya, Pakistan, Paraguay, Turkey, and the United Arab Emirates. Working in countries where governments

are vulnerable to terrorist financing, RLAs focus on money laundering and financial crimes and developing counterterrorism legislation that criminalizes terrorist acts, terrorist financing, and the provision of material support or resources to terrorist organizations. The RLAs also develop technical assistance programs for prosecutors, judges, and, in collaboration with DOJ's International Criminal Investigative Training Assistance Program (ICITAP), police investigators to assist in the implementation of new money laundering and terrorist financing procedures.

Also in 2008, OPDAT, AFMLS, and CTS met with and provided presentations to international visitors from more than 29 countries on AML/CTF topics. Presentations covered U.S. policies to combat terrorism, including legislation passed and pending at the time of the presentations, and issues raised in implementing new legislative tools, and the changing relationship of criminal and intelligence investigations. The USA PATRIOT Act, PATRIOT Improvement and Reauthorization Act, Intelligence Reform and Terrorism Prevention Act, Foreign Intelligence Surveillance Act, terrorist financing and material support statutes, and the Classified Information Procedures Act are among the significant pieces of legislation addressed. Of great interest to visitors is the balancing of civil liberties and national security issues, which is also addressed. When possible, CTS and U.S. Attorney's Offices bring trial attorneys or Assistant U.S. Attorneys with case or investigation experience with the visitors' countries to participate in the programs.

RLA Assistance in Bangladesh for CTF and to Develop a Career Prosecution Service. In March 2005, OPDAT placed its first RLA in South Asia at U.S. Embassy Dhaka with the goal of assisting the Government of Bangladesh in strengthening its AML/CTF regime, and improving the capability of its law enforcement agencies to investigate and prosecute complex financial and organized crimes. To assist in the development of a permanent career prosecution service in Bangladesh, OPDAT's RLA to Bangladesh arranged a study-tour program in January 2008 for eight high-level Bangladesh government officials to meet with and receive guidance from their counterparts in the Singapore Attorney General's Chambers in Singapore. This program is the first in a series of DOJ efforts designed to help Bangladesh develop a career prosecution service with a professionally selected and trained cadre of government prosecutors, similar to institutions like the U.S. Attorney's Office or Crown Prosecution Service, where career prosecutors are chosen on merit rather than political connections.

RLA Assistance for CTF in Indonesia. The OPDAT RLA program in Indonesia began in June 2005. In 2008, the RLA continued to engage the Attorney General's Terrorism and Transnational Crime Task Force (SATGAS), which OPDAT helped establish as an operational unit in 2006. The task force is responsible for prosecuting significant cases involving four key areas: terrorism, money laundering, trafficking in persons, and cyber crime. The SATGAS unit has yielded tangible results. In its first two years of operation, it successfully prosecuted 43 terrorists—including 26 Jamaah Islamiyah (JI) members and more than 40 trafficking-in-persons cases. The SATGAS unit has nationwide jurisdiction for such prosecutions, but also works with the local offices to promote such prosecutions. Over the course of 2008, the RLA conducted a number of regional training programs for SATGAS. These programs focused on providing substantive knowledge to local prosecutors concerning the task force's priorities while building relationships between the members of the task force and the prosecutors in the field. The RLA engaged the experienced members of SATGAS as fellow presenters in the trainings. The use of experienced Indonesian SATGAS prosecutors as instructors elicited a high level of engagement on the part of the local prosecutors. Due to Indonesia's physical size and SATGAS' national mandate, regional training and outreach is a key element in USG support for SATGAS. On September 26, 2008, Ambassador Hume and Attorney General Supandji signed a two-year extension agreement for USG support of the SATGAS unit.

RLA Assistance for CTF in Turkey. The OPDAT program in Ankara, Turkey, began in September 2006 and includes three prongs—anti-money laundering, terrorist financing, and PKK issues. In May, OPDAT's RLA to Turkey hosted a high level, three-person delegation from Turkey to Washington,

D.C., to discuss extradition, mutual legal assistance, and counterterrorism. In June, OPDAT's RLA to Turkey convened a conference on counterterrorism and extradition in Istanbul, Turkey. The purpose of the program was to exchange best practices on combating terrorism and discuss the basic legal requirements for extradition in terrorism and terrorism-related cases.

RLA Assistance for CTF in Kenya. OPDAT's RLA program in Kenya began in 2004. In 2008, the RLA continued to engage Government of Kenya partners—such as the Department of Public Prosecutions, Kenya's Anticorruption Commission, the Law Society of Kenya, and others—in a program that focuses on counterterrorist financing, anticorruption, and procedural reform.

RLA Assistance for CTF in Pakistan. Despite the difficult political climate in Pakistan, OPDAT launched its RLA program at U.S. Embassy Islamabad in September 2006. The RLA, to the extent possible, concentrated on assisting Pakistan in combating terrorist financing and money laundering, judicial reform, judicial security, and IPR violations. OPDAT deployed the current RLA to Islamabad in October 2008.

RLA Assistance for CTF in Paraguay. OPDAT's RLA program in Paraguay began in 2003, and now carries regional responsibilities in the Tri-Border Area of Paraguay, Argentina, and Brazil. In 2008, the RLA continued to encourage Paraguayan legislators to pass a revised draft Criminal Procedure Code, which is pending before the lower chamber of the legislature. The Paraguayan legislature has already passed a revised Penal Code that contains new money laundering, IPR, and trafficking in persons statutes; the new Penal Code will go into effect in June 2009. The RLA also discussed Paraguay's fulfillment of international commitments and passage of a CTF law. In addition, the RLA is working closely with the U.S. Agency for International Development (USAID) on plans to form, train, and coordinate the activities of a new Paraguayan money laundering task force. Specifically, USAID and the RLA are working on standardizing reports used by the various law enforcement agencies charged with investigating money laundering and financial crimes. The reports will be used by members of the task force to foster timely information sharing.

Counterterrorism/CTF Program in Azerbaijan. In conjunction with a visiting team, OPDAT held a four-day seminar for 18 prosecutors and police on detecting and fighting terrorism and its financing.

U.S. Study Tour for Romanian Delegation on Financial Investigations, Counterterrorism, and CTF. In November, OPDAT organized a series of meetings in Washington, D.C., for two officials from Romania's FIU. The focus of the program was to aid the Romanians in meeting relevant USG counterparts with same or similar counterterrorism and CTF responsibilities.

AML/CTF Training Courses in Serbia. From May to October, OPDAT conducted four training courses for Serbian prosecutors, police, and trial judges on prosecution and adjudication of money laundering and terrorist financing cases. The training courses focused on improving participants' knowledge of money laundering legislation, terrorist financing, available investigative techniques, and standards of proof. From May to September 2008, OPDAT conducted four additional training courses for prosecutors, police, and investigative judges on financial crimes investigations to enhance their capacity to detect and prosecute a variety of financial crimes.

Office of Technical Assistance (OTA), Treasury Department

The U.S. Department of the Treasury's Office of Technical Assistance (OTA) is located within the Office of International Affairs. OTA has five training and technical assistance programs: revenue policy and revenue administration, government debt issuance and management, budget policy and management, banking and financial services, and economic crimes (formerly financial enforcement). The economic crimes program offers technical assistance to combat money laundering, terrorist financing, and other financial crimes.

Sixty experienced intermittent advisors (IAs) and resident advisors (RAs) comprise the Economic Crimes Team (ECT). These advisors provide diverse expertise in the development of regimes for anti-money laundering and combating the financing of terrorism (AML/CTF), and the investigation and prosecution of complex financial crimes. ECT is divided into three regional areas, each of which is managed by a full-time RA: Europe and Asia, Africa and the Middle East, and the Americas.

OTA receives funding from direct appropriations from the U.S. Congress, from the U.S. Department of State's Bureau of International Narcotics and Law Enforcement (INL), the U.S. Department of Defense, U.S. Agency for International Development (USAID) country missions, and the Millennium Challenge Corporation (MCC).

Assessing Training and Technical Assistance Needs

The goal of OTA's economic crimes program is to build the capacity of host countries to prevent, detect, investigate, and prosecute complex international financial crimes by providing technical assistance in three primary areas: combating money laundering, terrorist financing, and other financial crimes; fighting organized crime and corruption; and building capacity for financial law enforcement entities.

Before initiating any training or technical assistance to a host government, an OTA economic crimes advisors conduct a comprehensive assessment to identify needs and to formulate a responsive assistance program. These needs assessments examine the legislative, regulatory, law enforcement, and judicial components of the various regimes, and include the development of technical assistance work plans to enhance a country's efforts to fight money laundering, terrorist financing, organized crime, and corruption. In 2008, OTA executed assessments in Oman, Algeria, West Bank, Lesotho, Egypt, Sao Tome and Principe, El Salvador, Guatemala, Honduras, Jamaica, Uruguay, Cambodia, Kyrgyzstan, Laos, and Turkmenistan.

AML/CTF Training

OTA specialists delivered AML/CTF courses to government and private sector stakeholders in a number of countries. Course topics included money laundering and financial crimes investigations; identification and development of local and international sources of information; operations and regulation of banks and nonbank financial institutions, including record keeping; investigative techniques; financial analysis techniques; forensic evidence; computer assistance and criminal analysis; interviewing; case development, planning, and organization; report writing; and, with the assistance of local legal experts, rules of evidence, search, and seizure, and asset seizure and forfeiture procedures.

In Africa and the Middle East, OTA delivered the financial investigative techniques (FIT) course in Malawi, Jordan and Egypt, and conducted regional FIT training for members of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) and the Intergovernmental Action Group against Money Laundering in West Africa (GIABA). OTA partnered with the U.S. Department of Justice's Office of Overseas Prosecutorial Development, Training and Assistance (OPDAT) to deliver seminars to investigators and prosecutors in Namibia and Jordan, promoting the use of the task force concept to investigate and prosecute complex financial crime cases. OTA presented a pilot analytical training course to Namibia's financial intelligence unit (FIU) and law enforcement analysts. OTA provided specialized cross border cash smuggling, trade-based money laundering, and investigative techniques training to Jordanian Customs officials.

OTA also collaborated with the U.S. Department of Homeland Security's (DHS) Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP) to deliver regional bulk cash smuggling training to member countries of the Middle East and North Africa Financial Action Task

Force (MENA-FATF) in Jordan. In collaboration with USAID, OTA provided training for Jordanian insurance industry personnel and regulators in AML/CTF compliance programs. OTA provided training to Namibian law enforcement officials, prosecutors, and casino regulators, and provided training and technical assistance to banking, securities and insurance regulators in Namibia, Jordan and Egypt as well as at a GIABA-sponsored banking regulator workshop in the Gambia.

OTA held a government executive AML/CTF seminar for officials in Sao Tome and Principe. In Lesotho, OTA provided a long-term IA to work with Lesotho's revenue authority in establishing a criminal investigation and intelligence department to address tax evasion, much of which is related to trade-based money laundering. In Tunisia, OTA provided an RA to the African Development Bank (AfDB) to establish an antifraud and corruption department, mentor investigators, establish training programs, develop procedures for an antifraud hot line, and set up a case management system. The advisor also co-chaired an internal AfDB committee tasked with the development of the Bank's AML/CTF strategy implementation plan.

Through the MCC, OTA placed an RA in Sao Tome and Principe to work with customs authorities to modernize operations. Work focuses on passing an internationally compliant customs code, installing a modern automated system to improve the processing, transparency, and security of goods moving through the seaport and airport, and improving infrastructure and capacity to execute customs operations, including inspection and countersmuggling. OTA also sponsored officials from Sao Tome and Principe to attend the regional FIT training course in Cote d'Ivoire.

In Asia, OTA conducted FIT training in Afghanistan, Cambodia, Laos, and Vietnam. OTA funded officials from Vietnamese law enforcement agencies and FIU for a study and orientation tour of the Philippines' FIU and law enforcement agencies. OTA also conducted several training sessions for Philippine border control agencies on bulk cash smuggling. In Central Asia, OTA provided training and mentoring assistance to law enforcement agencies and banking institutions in Kyrgyzstan, and financial analysis techniques training to FIU staff from Kyrgyzstan and Kazakhstan.

In Europe, OTA teams delivered a variety of technical assistance products, including FIT training in the northern part of Cyprus and Georgia's revenue service; financial analysis techniques training to the Armenian FIU; and training for Macedonian banking supervisors. OTA provided a regional cybercrime workshop in Poland for FIUs from ten countries in Eastern Europe and the Eurasian Group on Combating Money Laundering and the Financing of Terrorism (EAG). OTA also funded officials from law enforcement agencies and the Kyrgyz FIU for a study and orientation tour of Poland's FIU and law enforcement agencies. OTA's RA to the secretariat of the EAG in Moscow continued to assist that body to develop operational standards in strategically important areas related to the Financial Action Task Force (FATF) recommendations.

In the Americas, OTA delivered technical assistance in Chile, Ecuador, El Salvador, Guatemala, Haiti, Honduras, Mexico, Paraguay, and Uruguay during 2008. In Chile, OTA continued to provide technical assistance to the Chilean national gaming authority in the supervision of casinos and their risks related to money laundering and terrorist financing. OTA provided financial analysis techniques course (FATC) training to the analysts of Ecuador's and Mexico's FIUs. OTA also worked closely with the Ecuadorian FIU to plan in financial investigative techniques, and in gaming sector supervision for money laundering and terrorist financing risk. OTA provided four iterations of FIT training to Mexico's FIU, and one at the International Law Enforcement Training Academy in El Salvador for participants from El Salvador and Guatemala. OTA also worked closely with the Mexican tax authority to provide AML/CTF training to its money service businesses supervisors.

OTA advisors presented its four-week criminal investigations training program for two newly established investigation units in Honduras, and provided assistance focused on developing capacity within each unit to conduct investigations and implement case management systems. In Haiti, OTA initiated technical assistance to develop a financial crimes unit and train its personnel, prosecutors and

judges. OTA presented the FATC for staff of the FIU and continued technical assistance with drafting a new and revised criminal code, drafting criminal provisions of the Haitian tax code, and mentoring of active cases.

In Paraguay, OTA's RA continued to work with the customs authority to stand up an internal investigations unit with MCC funding. In Uruguay, OTA provided an advisor who worked with the Uruguayan FIU to present a workshop on prevention and detection of money laundering and terrorist financing. OTA continued to offer a train-the-trainer course so that the basic skills taught in investigative courses can be passed on by the recipients to their agency colleagues.

Financial Intelligence Units

OTA placed a new RA in Kabul in late 2008 to continue to assist in the development of an operational FIU within the Da Afghanistan Bank, Afghanistan's central bank, and the licensing of hawaladars in Afghanistan. In January 2008, OTA established a new resident technical assistance project to stand up an FIU in Kosovo. RAs in Montenegro and Serbia, and intermittent advisors in Armenia, Georgia, and Kyrgyzstan, delivered technical assistance to streamline and enhance host governments' FIUs. In Georgia, this assistance included information technology (IT) development. In Paraguay, OTA continued to advise the FIU on its analytical and IT operational capacity.

In Namibia, Ethiopia, Algeria, Sao Tome and Principe, Malawi, and Jordan, advisors engaged with the respective central banks to establish and develop fully functional FIUs. In Malawi, OTA purchased IT equipment and software for the newly-established FIU, funded the training of FIU staff on the use of analytical and database software, and provided training to FIU staff. In Namibia, the RA assisted in drafting implementing regulations for the FIU, and funded UN officials to conduct an FIU IT assessment resulting in the acquisition of UN-developed software to support its database functions.

In Jordan, the OTA RA worked with the FIU director to prepare for a mutual evaluation and engagement in all OTA-sponsored training with FIU stakeholders. The RA also served as the coordinator for the expenditure of INL funds for the physical development of the FIU, including IT equipment, and database and IT system development. In Kuwait, OTA, with OPDAT and the U.S. FIU, Financial Crimes Enforcement Network (FinCEN), conducted an FIU workshop. In Sao Tome and Principe, OTA executed a terms of reference with the government to assist in the revision of its AML legislation, and to establish an FIU and an overall AML/CTF regime.

OTA continued its work with the FIUs of Guatemala, El Salvador, and Honduras by providing training seminars in the area of Financial Investigative Techniques and Financial Analysis. In Ecuador and Mexico, OTA provided a Financial Analysts Training Course for analysts of those nations' FIUs. In addition, OTA continued its work in the IT area, assisting the Ecuador FIU in its efforts to streamline the process of receiving reports from obligated entities. In Uruguay, OTA collaborated with the FIU by providing a speaker for a seminar focused on AML/CTF issues.

Casinos and Gaming

In the casino gaming group (CGG), OTA experts from its economic crimes program has provided technical assistance to the international community in the areas of gaming industry regulation since 2000. The program provides assistance in the drafting of gaming legislation and implementing regulations. The CGG also includes training for gaming industry regulators, including FIU personnel, to develop the capacity for implementing AML programs, conducting pre-licensing investigations, and auditing and inspecting casino operations and all games of chance. In addition, The CGG organized and conducted two advanced technical workshops in Las Vegas involving Chilean regulators. In 2008, the CGG assessed the gaming regulatory systems and AML programs for the governments of Kosovo, Bosnia-Herzegovina, and Namibia, and assisted Kosovo in major revisions to its gaming laws. A

member of the CGG presented on AML issues and the casino environment at a conference sponsored by Panama's gaming commission.

In September, 40 regulators, analysts, and financial investigators from Mexico's tax authority, FIU, and commission for banks and securities gathered in Mexico City for a two-day workshop on money service businesses oversight, regulation, and examination given by the tax authorities and OTA.

Insurance

OTA provides technical assistance to foreign governments to protect insurance systems from money laundering, terrorist financing, and fraud. OTA initiated new projects in Egypt, Namibia, and Central America. Work with the Egyptian insurance regulatory authority concentrates on insurance sector compliance with AML/CTF laws requiring inspections by government regulators and will subsequently focus on antifraud measures. Insurance assistance provided to Namibia included inspection procedures to regulate insurance companies' AML compliance. Training was provided to both government officials and the insurance industry. OTA presented on AML/CTF risks in the insurance sector at a regional conference hosted by Panama. In Paraguay, OTA continued to focus on curbing money laundering by assisting government regulators with regulatory review, training, and compliance inspections of insurance companies. The Paraguay project concluded with a regional conference in Asuncion devoted to the prevention and detection of money laundering risk in the insurance sector. The conference included participation from 11 countries and a presentation by the U.S. Internal Revenue Service.

Regional and Resident Advisors (RA)

OTA RAs continued international support in the areas of money laundering and terrorist financing. In February, OTA moved its Africa and Middle East Regional Advisor, previously based in Pretoria, South Africa, to Cairo, Egypt, resulting in increased support for programs in the Middle East and North Africa. An RA posted in Namibia continued assisting with FIU development. OTA upgraded its economic crimes advisor position in Sao Tome and Principe to a full-time residency to better implement a customs modernization project. Supported by long-term Advisors with customs and AML expertise, the RA provided technical assistance to strengthen core responsibilities and infrastructure. OTA extended the presence of a RA to work with Jordan's law enforcement, regulatory, and customs authorities. OTA closed out its RA program in Zambia in August.

OTA's Regional Advisor for Europe and Asia participated as one of two delegates from the United States at the Asia-Pacific Economic Cooperation (APEC) "Seminar on Securing Remittance and Cross Border Payment from Terrorist Use" held in Jakarta, Indonesia, in October. OTA continued its RA to the secretariat of the EAG, and RAs in Montenegro and Serbia focused on supporting national efforts against financial crimes.

OTA's RA in Paraguay continued to provide assistance to develop the internal affairs unit within the customs administration, including assistance with the identification, vetting, and training of personnel, and the provision of workplaces. The customs unit has made significant progress in investigating matters under its jurisdiction. OTA closed out its resident economic crimes advisor program in Argentina in June.

Treaties and Agreements

Treaties

Mutual Legal Assistance Treaties (MLATs) allow generally for the exchange of evidence and information in criminal and ancillary matters. In money laundering cases, they can be extremely useful as a means of obtaining banking and other financial records from our treaty partners. MLATs, which are negotiated by the Department of State in cooperation with the Department of Justice to facilitate cooperation in criminal matters, including money laundering and asset forfeiture, are in force with the following countries: Antigua and Barbuda, Argentina, Australia, Austria, the Bahamas, Barbados, Belgium, Belize, Brazil, Canada, Cyprus, Czech Republic, Dominica, Egypt, Estonia, France, France with respect to its overseas departments (French Guiana, Guadeloupe and Martinique) and collectivities (French Polynesia and Saint Martin), Greece, Grenada, Hungary, India, Israel, Italy, Jamaica, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malaysia, Mexico, Morocco, the Netherlands, the Netherlands with respect to its Caribbean overseas territories (Aruba and the Netherlands Antilles), Nigeria, Panama, the Philippines, Poland, Romania, Russia, South Africa, South Korea, Spain, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Switzerland, Thailand, Trinidad and Tobago, Turkey, Ukraine, the United Kingdom, the United Kingdom with respect to its Caribbean overseas territories (Anguilla, the British Virgin Islands, the Cayman Islands, Montserrat, and the Turks and Caicos Islands), and Uruguay. The United States also has agreements in place for cooperation in criminal matters with Hong Kong (SAR) and the Peoples Republic of China (PRC). Mutual legal assistance agreements have been signed by the United States but not yet brought into force with the European Union and the following countries: Bermuda, Bulgaria, Colombia, Finland, Germany, Ireland, Sweden, and Venezuela. The United States is actively engaged in negotiating additional MLATs with countries around the world. The United States has also signed and ratified the Inter-American Convention on Mutual Legal Assistance of the Organization of American States and the United Nations Convention against Corruption.

Agreements

In addition to MLATs, the United States has entered into executive agreements on forfeiture cooperation, including: (1) an agreement with the United Kingdom providing for forfeiture assistance and asset sharing in narcotics cases; (2) a forfeiture cooperation and asset sharing agreement with the Kingdom of the Netherlands; and (3) a drug forfeiture agreement with Singapore. The United States has asset sharing agreements with Canada, the Cayman Islands (which was extended to Anguilla, British Virgin Islands, Montserrat, and the Turks and Caicos Islands), Colombia, Ecuador, Jamaica, and Mexico.

Treasury's Financial Crimes Enforcement Network (FinCEN) has a Memorandum of Understanding (MOU) or an exchange of letters in place with other financial intelligence units (FIUs) to facilitate the exchange of information between FinCEN and the respective country's FIU. FinCEN has an MOU or an exchange of letters with the FIUs in Albania, Argentina, Aruba, Australia, Belgium, Bulgaria, Canada, Cayman Islands, Chile, Croatia, Cyprus, France, Guatemala, Indonesia, Italy, Japan, Macedonia, Malaysia, Mexico, Montenegro, the Netherlands, Netherlands Antilles, Panama, Paraguay, Philippines, Poland, Romania, Russia, Singapore, Slovenia, South Africa, South Korea, Spain, the Money Laundering Prevention Commission of Taiwan and the United Kingdom.

Asset Sharing

Pursuant to the provisions of U.S. law, including 18 U.S.C. § 981(i), 21 U.S.C. § 881(e)(1)(E), and 31 U.S.C. § 9703(h)(2), the Departments of Justice, State, and Treasury have aggressively sought to encourage foreign governments to cooperate in joint investigations of narcotics trafficking and money laundering, offering the possibility of sharing in forfeited assets. A parallel goal has been to encourage spending of these assets to improve narcotics related law enforcement. The long-term goal has been to encourage governments to improve asset forfeiture laws and procedures so they will be able to conduct investigations and prosecutions of narcotics trafficking and money laundering, which include asset forfeiture. The United States and its partners in the G-8 are currently pursuing a program to strengthen asset forfeiture regimes. To date, Canada, Cayman Islands, Hong Kong, Jersey, Liechtenstein, Luxembourg, Switzerland, and the United Kingdom have shared forfeited assets with the United States.

From 1989 through December 2008, the international asset sharing program, administered by the Department of Justice, shared $229,580,918 with foreign governments that cooperated and assisted in the investigations. In 2008, the Department of Justice transferred $499,913.50 in forfeited proceeds to Canada. Prior recipients of shared assets include: Anguilla, Antigua and Barbuda, Argentina, the Bahamas, Barbados, British Virgin Islands, Canada, Cayman Islands, Colombia, Costa Rica, Dominican Republic, Ecuador, Egypt, Greece, Guatemala, Guernsey, Honduras, Hong Kong (SAR), Hungary, Indonesia, Isle of Man, Israel, Jordan, Liechtenstein, Luxembourg, Netherlands Antilles, Paraguay, Peru, Romania, South Africa, Switzerland, Thailand, Turkey, the United Kingdom, and Venezuela.

From Fiscal Year (FY) 1994 through FY 2008, the international asset-sharing program administered by the Department of Treasury shared $28,025,669 with foreign governments that cooperated and assisted in successful forfeiture investigations. In FY 2008, the Department of Treasury transferred $218,657 in forfeited proceeds to Canada ($145,659), Guernsey ($18,690), and Palau ($54,308). Prior recipients of shared assets include: Aruba, Australia, the Bahamas, Cayman Islands, Canada, China, Dominican Republic, Egypt, Guernsey, Honduras, Isle of Man, Jersey, Mexico, Netherlands, Nicaragua, Panama, Portugal, Qatar, St. Vincent & the Grenadines, Switzerland, and the United Kingdom.

Multi-Lateral Organizations & Programs

The Financial Action Task Force (FATF) and FATF-Style Regional Bodies (FSRBs)

The Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. The FATF was created in 1989 and works to generate legislative and regulatory reforms in these areas. The FATF currently has 34 members, comprising 32 member countries and territories and two regional organizations, as follows: Argentina, Australia, Austria, Belgium, Brazil, Canada, Denmark, Finland, France, Germany, Greece, Hong Kong, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, The Netherlands, New Zealand, Norway, The Peoples Republic of China, Portugal, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United

Kingdom, the United States, the European Commission and the Gulf Cooperation Council. FATF admitted The Peoples Republic of China in June 2007.

There are also a number of FATF-style regional bodies that, in conjunction with the FATF, constitute an affiliated global network to combat money laundering and the financing of terrorism.

The Asia Pacific Group (APG)

The Asia Pacific Group (APG) was officially established in February 1997 at the Fourth (and last) Asia/Pacific Money Laundering Symposium in Bangkok as an autonomous regional anti-money laundering body. The 36 APG members are as follows: Afghanistan, Australia, Bangladesh, Brunei Darussalam, Burma, Cambodia, Canada Chinese Taipei, Cook Islands, Fiji, Hong Kong, India, Indonesia, Japan, Laos, Macau, Malaysia, Maldives, Marshall Islands, Mongolia, Nauru, Nepal, New Zealand, Niue, Pakistan, Palau, Philippines, Samoa, Singapore, Solomon Islands, South Korea, Sri Lanka, Thailand, Tonga, Timor Este, United States, Vietnam, and Vanuatu. Papua New Guinea became the 39th member of the APG in December 2008.

The Caribbean Financial Action Task Force (CFATF)

The Caribbean Financial Action Task Force (CFATF) was established in 1992. CFATF has thirty members: Anguilla, Antigua & Barbuda, Aruba, The Bahamas, Barbados, Belize, Bermuda, British Virgin Islands, Cayman Islands, Costa Rica, Dominica, Dominican Republic, El Salvador, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Montserrat, Netherlands Antilles, Nicaragua, Panama, St. Kitts & Nevis, St. Lucia, St. Vincent & the Grenadines, Suriname, Trinidad & Tobago, Turks & Caicos Islands, and Venezuela.

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL)

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) was established in 1997 under the acronym PC-R-EV. MONEYVAL is comprised of twenty-eight permanent members, two temporary, rotating members and one active observer. The permanent members are Albania, Andorra, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Georgia, Hungary, Latvia, Liechtenstein, Lithuania, Moldova, Malta, Monaco, Montenegro, Poland, Romania, Russian Federation, San Marino, Serbia, Slovakia, Slovenia, the Former Yugoslav Republic of Macedonia, and Ukraine. The active observer is Israel. Temporary members, designated by the FATF for a two-year membership, are France and the Netherlands.

The Eastern and South African Anti Money Laundering Group (ESAAMLG)

The Eastern and South African Anti Money Laundering Group (ESAAMLG) was established in 1999. Fourteen countries comprise its membership: Botswana, Kenya, Lesotho, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Swaziland, Tanzania, Uganda, Zambia, and Zimbabwe.

The Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG)

The Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) was established on October 6, 2004 and has seven members: Belarus, China, Kazakhstan, Kyrgyzstan, the Russian Federation, Uzbekistan, and Tajikistan.

The Financial Action Task Force on Money Laundering in South America (GAFISUD)

The Financial Action Task Force on Money Laundering in South America (GAFISUD) was formally established on 8 December 2000 by the nine member states of Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Mexico, Paraguay, Peru and Uruguay.

The Groupe Intergouvernemental d'Action contre le Blanchiment en Afrique/ Intergovernmental Action Group against Money Laundering in West Africa (GIABA)

The Groupe Intergouvernemental d'Action contre le Blanchiment en Afrique/Intergovernmental Action Group against Money Laundering in West Africa (GIABA) consists of 15 countries: Benin, Burkina Faso, Cape Verde, Côte d'Ivoire, Gambia, Ghana, Guinea Bissau, Guinea (Conakry), Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, and Togo.

The Middle East and North Africa Financial Action Task Force (MENAFATF)

The Middle East and North Africa Financial Action Task Force (MENAFATF) consists of 16 members: Algeria, Bahrain, Egypt, Jordan, Kuwait, Lebanon, Mauritania, Morocco, Oman, Qatar, Saudi Arabia, Sudan, Syria, Tunisia, United Arab Emirates, and Yemen.

The Egmont Group of Financial Intelligence Units

The Egmont Group began in 1995 as a collection of a small handful of national entities—today referred to as financial intelligence units (FIUs)—seeking to explore ways to cooperate internationally among themselves. The FIU concept is now an important component of the international community's approach to combating money laundering and terrorist financing. To meet the standards of Egmont membership, an FIU must be a centralized unit within a nation or jurisdiction to detect criminal financial activity and ensure adherence to laws against financial crimes, including terrorist financing and money laundering. The Egmont Group recognizes four types of FIUs: the administrative model, the judicial or prosecutorial model, the law enforcement model, and the hybrid/mixed model.

The Egmont Group has grown dramatically from 14 units in 1995 to a recognized membership of 107 FIUs in 2008. The current 107 includes two new Egmont members, the FIUs of Moldova and the Turks and Caicos, as well as the removal of Bolivia's FIU from the Egmont Group. Today, the Egmont Group is a major player in the world of financial intelligence expertise and information sharing. It vigorously promotes cooperation in the fight against money laundering and financing of terrorism worldwide and fosters the implementation of domestic, regional, and international programs in the area.

Significant achievements of the Egmont Group for 2007/2008 include: an increased focus on the fight against corruption; a revised definition of what constitutes an Egmont Group FIU, which includes a strict and mandatory terrorist financing component; ensuring all current and future members meet the

new FIU definition; a revised working relationship with the Financial Action Task Force (FATF); and holding four major meetings in Bermuda, Republic of Korea, Ukraine, and Chile.

The goal of the Egmont Group is to provide a forum for FIUs around the world to improve support to their respective governments in the fight against money laundering, terrorist financing, and other financial crimes. This support includes expanding and systematizing the exchange of financial intelligence information, improving expertise and capabilities of personnel employed by such organizations, and fostering better and more secure communication among FIUs through the application of technology.

The Egmont Group's secure Internet system permits members to communicate with one another via secure e-mail, requesting and sharing case information as well as posting and assessing information on typologies, analytical tools and technological developments. The U.S. FIU, called the Financial Crimes and Enforcement Network (FinCEN), on behalf of the Egmont Group, maintains the Egmont Secure Web (ESW). Currently, there are 106 Egmont Group FIUs (with the exception of Niue) connected to the ESW. FinCEN and the European Union's FIU.net Bureau reached an agreement on allowing a connection between the ESW and FUI.net, so that FIUs using either of those secured networks can exchange information across the two of them.

The Egmont Group is organizationally structured to meet the challenges of the volume of membership and its workload. The Egmont committee, a group of 14 members, is an intermediary group between the 107 heads of member FIUs and the five Egmont working groups. This Committee addresses the administrative and operational issues facing the Egmont Group and is comprised of seven permanent members and seven regional representatives based on continental groupings (i.e., Asia, Europe, the Americas, Africa, and Oceania).

In addition to the committee, there are five working groups: legal, operational, training, information technology, and outreach. The legal working group reviews the candidacy of potential members and handles all legal aspects and matters of principle within the Egmont Group. The training working group looks at ways to communicate more effectively, identifies training opportunities for FIU personnel, and examines new software applications that might facilitate analytical work. The outreach working group concentrates on expanding and developing the FIU global network by identifying countries that have established or are establishing FIUs. This working group is responsible for making initial contact with potential candidate FIUs, and conducts assessments to determine if an FIU is ready for Egmont membership. The operational working group is designed to foster increased cooperation among the operational divisions of the member FIUs and coordinate the development of studies and typologies-using data collected by the FIUs-on a variety of subjects useful to law enforcement. The information technology (IT) working group promotes collaboration and information sharing on IT matters among the Egmont membership, in particular looking to increase the efficiency in the allocation of resources and technical assistance regarding IT systems. The committee and the working groups meet at a minimum three times per year, including the annual plenary session.

In July of 2007, the Egmont Group established a Secretariat office to meet an ever-growing demand in terms of volume and complexity. In 2007-2008, the primary focus of the Egmont Secretariat has been on operational matters, including developing its financial and administrative procedures. Its future work will be focused on developing and enhancing the cooperative relationship between the Egmont Group and other international anti-money laundering and combating financing of terrorism (AML/CTF) organizations. It will ensure that Egmont preserves its reputation in both the public and private sectors by emphasizing the importance of meeting and maintaining uniform standards of quality by all FIUs. The Egmont secretariat is now established in Toronto, Canada, and is headed by an Executive Secretary, appointed by the heads of FIUs, and reports directly to them through the Egmont committee.

In December 2008, the Egmont Group expelled Bolivia's FIU from its membership, due to a lack of terrorism financing legislation in Bolivian law. To regain Egmont membership, Bolivia must reapply and provide written evidence of its FIU's compliance with Egmont FIU definitions and requirements. The remaining 107 members of the Egmont Group are Albania, Andorra, Anguilla, Antigua and Barbuda, Argentina, Armenia, Aruba, Australia, Austria, Bahamas, Bahrain, Barbados, Belarus, Belgium, Belize, Bermuda, Bosnia and Herzegovina, Brazil, British Virgin Islands, Bulgaria, Canada, Cayman Islands, Chile, Colombia, Cook Islands, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Dominica, Egypt, El Salvador, Estonia, Finland, France, Georgia, Germany, Gibraltar, Greece, Grenada, Guatemala, Guernsey, Honduras, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Isle of Man, Israel, Italy, Japan, Jersey, Latvia, Lebanon, Liechtenstein, Lithuania, Luxembourg, Macedonia, Malaysia, Malta, Marshall Islands, Mauritius, Mexico, Moldova, Monaco, Montenegro, Netherlands, Netherlands Antilles, New Zealand, Nigeria, Niue, Norway, Panama, Paraguay, Peru, Philippines, Poland, Portugal, Qatar, Romania, Russia, San Marino, Serbia, Singapore, Slovakia, Slovenia, South Africa, South Korea, Spain, St. Kitts and Nevis, St. Vincent and the Grenadines, Sweden, Switzerland, Syria, Taiwan, Thailand, Turkey, Turks and Caicos, Ukraine, United Arab Emirates, United Kingdom, United States, Vanuatu, and Venezuela.

The Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Group of Experts to Control Money Laundering

The Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) is responsible for combating illicit drugs and related crimes, including money laundering. In 2008, CICAD continued to carry out its activities in anti-money laundering and combating the financing of terrorism (AML/CTF) throughout Latin America and the Caribbean. CICAD's AML/CTF training programs seek to improve and enhance the knowledge and capabilities of judges, prosecutors, public defenders, law enforcement agents, and financial intelligence unit (FIU) analysts. The U.S. Department of State Bureau of International Narcotics and Law Enforcement (INL) provided full or partial funding for many of the CICAD training programs in 2008.

CICAD's Group of Experts to Control Money Laundering met twice this year, once in Washington, D.C., in July, and once in Mexico City, Mexico, in October. The first meeting was held specifically for the asset forfeiture and FIU-law enforcement coordination and integration sub-groups. Experts at the second meeting discussed and approved a best practices manual on the management of seized and forfeited assets in Latin America, which was initially discussed during the subgroups meeting in July. As a next step, CICAD plans to implement the asset forfeiture best practices manual by offering technical assistance to interested OAS member states. The initial set of countries chosen for the first phase of this project includes Uruguay, Chile, and Argentina.

With participation from the UN Office on Drugs and Crime (UNODC), CICAD held money laundering mock trial training sessions in 2008 in four countries: Mexico (39 participants), Paraguay (28 participants), Uruguay (30 participants), and Venezuela (29 participants). The mock trial sessions provided specialists from these countries an opportunity to simulate the steps involved in investigating and prosecuting real money laundering cases. This hands-on learning method takes place over four days, the first of which consists of international expert presentations, and the following days consist of the trial itself. Over the course of the mock trial, teams of investigators, prosecutors, financial analysts, and judges follow a money laundering case from the initial probes to detect illegal activity, through the preparation of an indictment and, finally, to trial. In addition to the mock trials, CICAD offered workshops for judges and prosecutors in Mexico (39 participants), Venezuela (65 participants), and Guatemala (44 participants). The events in Mexico and Guatemala, both the mock trials and the

workshop for judges and prosecutors, occurred with the assistance of financial and organizational support from the U.S. Embassy's narcotics affairs sections in both countries.

In 2008, CICAD's AML section supported the development and implementation of an online money laundering case classification system, called the Typologies Database, that stores, classifies, organizes, updates, and retrieves information on case histories, common money laundering practices, techniques to detect them, and the prosecutorial methods to take cases to trial. With its interactive functions and hemispheric scope, the database is the first of its kind in the world and is now operative on CICAD's website (www.cicad.oas.org/tipologias). It allows investigators to search the database for cases similar to those they are investigating. This user-friendly Internet application permits authorized users to load, validate, and publish new typologies based on the latest cases analyzed by law enforcement agencies.

CICAD's AML section held two events to complement the database application. In Ecuador, CICAD offered a regional seminar on money laundering typologies, which included representatives from eight GAFISUD (Grupo de Acción Financiera Internacional de Sudamérica or Financial Action Task Force of South America) member states. At the seminar, participants identified and defined the typologies, terminology, and classification criteria in the database. The final document from this seminar will soon be published online as a shared reference tool.

The second event was held in Bogotá, Colombia, where the FIU organized a workshop to train its staff to use and begin uploading cases into the database. As a result of this initiative, CICAD's AML section developed two documents on typologies in coordination with the FIU of Colombia: one on terrorist financing that includes eight cases and a second one on money laundering that includes 11 cases.

CICAD's AML section also supported the development and evaluation of a software application to capture, store, query, analyze, and manage information from Uruguay's FIU. The goal is to expand the use of this software, currently in "Beta" version, to other countries.

In cooperation with Spain's University of Salamanca, CICAD is working on an online degree in anti-money laundering, aimed at law enforcement agents, prosecutors, judges, FIU analysts, and bankers. This program would be taught by Spanish money laundering experts, and consist of three modules at the basic, intermediary, and advanced levels.

CICAD acquired computer hardware and projectors as a follow-up to a train-the-trainer program in Costa Rica. CICAD purchased one laptop and one projector for Costa Rica this year, in order to advance the program in that country.

CICAD's AML section also worked with the Inter-American Committee against Terrorism (CICTE), participating in two of their CTF seminars, one in Antigua & Barbuda and the other in Brazil.

Pacific Anti-Money Laundering Program (PALP)

The Pacific Anti-Money Laundering Program (PALP) was launched in September 2006. PALP is a joint initiative between the UN Office on Drugs and Crime (UNODC) and the U.S. Department of State. PALP was conceived by and is funded by the U.S. Department of State's Bureau for International Narcotics and Law Enforcement Affairs. PALP is a four-year regional technical assistance and training program designed to assist the 14 members of the Pacific Islands Forum that are not also members of the Financial Action Task Force (FATF) in establishing, enhancing, and implementing their anti-money laundering and combating the financing of terrorism (AML/CTF) regimes. The 14 members of the Pacific Islands Forum that receive PALP assistance are the Cook Islands, the Federated States of Micronesia, Fiji, Kiribati, the Marshall Islands, Nauru, Niue, Palau, Papua New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu, and Vanuatu.

During it first two years, PALP was coordinated and administered by the Pacific Islands Forum Secretariat. In September 2008 the coordination role was assumed by the UNODC Global Programme against Money Laundering, Proceeds of Crime and Financing of Terrorism (GPML).

The goal of PALP training and technical assistance is to support participating jurisdictions to comply with international FATF standards and relevant UN conventions and UN Security Council resolutions. PALP is essentially a regional outreach program, utilizing experienced mentors based in host countries to assist with legal, law enforcement, regulatory, and financial intelligence unit (FIU) development. In 2008, PALP provided assistance on a wide range of AML/CTF issues, including legislative drafting, capacity building, and case support. Regional and bilateral training was also conducted for prosecutors and law enforcement officers and other key stakeholders.

Mentoring

PALP uses resident and intermittent mentors to deliver regional and bilateral training and advice for establishing viable AML/CTF regimes. PALP currently has mentors in the legal and law enforcement fields in Tonga and Palau, respectively, as well as intermittent mentors for FIUs and regulatory issues. In the first half of 2008, a second law enforcement mentor was based in Vanuatu. Although PALP mentors are based in their host countries, they are able to respond to requests for assistance from any of 14 participating countries and travel to those jurisdictions, often for periods up to one month or more at a time.

The PALP mentoring program supports multiple AML/CTF elements. Due to their extensive experience, PALP mentors advise officials on applying and adapting international standards to fit local situations. PALP mentors provide on-the-job training and work with local officials to ensure that they have sufficient capacity to implement the member country's AML/CTF regime. The amount of time spent in-country also offers a useful opportunity for mentors to assess the situation on the ground with regard to AML/CTF regime compliance and vulnerabilities.

Reviews were conducted by the PALP intermittent FIU mentor in the Marshall Islands, Palau, Tonga, and Vanuatu in 2007. Those reviews resulted in vigorous follow-up by the PALP legal and law enforcement mentors, which included the identification of resources to ensure effective follow-up and implementation of the recommendations derived from the FIU reviews.

Part of the PALP strategy aimed at building national capacity in AML/CTF systems entails efforts to strengthen the role of national AML/CTF committees at the policy level. In 2008, the PALP mentors played vital roles in providing support and advice to the national AML/CTF committees of several jurisdictions in the region, including Tonga, Cook Islands, Fiji, Palau, the Marshall Islands, the Solomon Islands, and Vanuatu.

Legislative Drafting

Vanuatu. Drafts have been provided to the authorities in Vanuatu for border currency reporting legislation and amendments to the Money Laundering and Proceeds of Crime Act identified in the last mutual evaluation by the Asia/Pacific Group on money laundering (APG). These bills are currently awaiting passage at the next sitting of Parliament in March 2009. Additional assistance will be provided in drafting legislation and regulations to remedy deficiencies discussed in the recent mutual evaluation report.

Tonga. Legislative drafting support was provided by preparing drafts for amendments to the Money Laundering and Proceeds of Crime Act and the Transnational Crimes Act as it relates to terrorist financing. Risk-based regulations have also been provided. These draft bills await cabinet approval and passage in the House of Assembly in June of 2009.

The Solomon Islands. Drafts have been provided for border currency reporting and FIU legislation. Continuing support will be provided in 2009 for other legislation.

The Cook Islands. Drafts have been provided for a suite of legislation and regulations, including border currency reporting legislation, FIU legislation, and civil forfeiture and risk-based AML/CTF regulations. These drafts await cabinet approval and passage in the House of Assembly in 2009.

Palau. Risk-based regulations have been drafted to meet the recommendations following a mutual evaluation. These regulations await approval of Congress. The PALP financial mentor who started in Palau in February 2008 has trained and worked with Palauan customs, police, and airport security agencies to identify potential bulk currency smugglers and methods employed by bulk currency smuggler. Palauan agencies have identified and made six bulk currency seizures in 2008. The mentor continues to assist law enforcement agencies enhance investigation techniques.

Republic of the Marshall Islands. Drafts have been prepared for border currency reporting, amendments to terrorist financing legislation, and amendments to the Banking Act. Risk-based regulations have also been provided. These drafts of legislation, amendments, and regulations await passage in the Parliament in 2009. Further assistance will be offered in 2009 to all beneficiaries in the support of legislative assistance.

Capacity Building Initiatives

In 2008 PALP provided technical assistance and training workshops at the regional, sub-regional and national levels for law enforcement, customs officials, and prosecutors. PALP mentors developed a border currency smuggling (BCS) training to implement international standards under FATF Special Recommendation IX. This program was first presented in Palau to members of Palauan customs, immigration, and airport security. PALP then expander this BCS training program by working in conjunction with the Oceania Customs Organization and the Australian Attorney General's Anti-Money Laundering Assistance Team (AMLAT). BCS training will be presented to the countries in the region at first on a bilateral basis and then via sub-regional and regional training. This training has been presented in Palau, Fiji, and the Solomon Islands.

PALP mentors conducted a pilot training in Palau to address basic law enforcement skills in report and affidavit writing. This training was delivered to members of the Palauan national police, customs and marine police. The success of this training has resulted in the development of a more advanced basic law enforcement skills training to include country laws and law enforcement authorities, report writing, interview techniques, evidence collection and processing, affidavits, court orders, subpoenas, executions of search warrants, and court room demeanor. This will be a two-part training initiative delivered to countries starting in 2009. The first part will be classroom-based and involve theory and practical exercises. The second part will be in the field, working through an investigation, and culminating in a mock trial.

In August 2008 PALP conducted a money laundering workshop in the Cook Islands with participants from the Cook Island FIU, national police, customs, tax and revenue, banking commission, and from some private banks. This workshop provided training on investigative techniques for investigation of money laundering.

PALP works in close cooperation with the APG in order to coordinate delivery of technical assistance and training to jurisdictions that are both APG members and PALP participants. The PALP law enforcement mentor made several presentations during the APG annual 2008 typologies workshop in Colombo, Sri Lanka. The presentations covered investigative techniques, letters of credit and basic charting techniques.

In June 2008, the PALP hosted a prosecutors' workshop on money laundering, and terrorist financing in Auckland, New Zealand. Twenty-two prosecutors from the Marshall Islands, Federated States of Micronesia, Palau, Papua New Guinea, Solomon Islands, Tonga, Fiji, Vanuatu, Samoa, the Cook Islands, Kiribati, and Tuvalu participated in this training. The workshop was funded and conducted by PALP. Additional experts from Hong Kong and the U.S. Department of Justice assisted in the presentation of the workshop. The course, which ran for one week, used a real case to demonstrate ways to take a money laundering case from investigation to the enforcement of a confiscation order and covered the following areas: investigation of money laundering and proceeds of crime; freezing and/or restraining of assets; management receivership orders; money laundering indictments; confiscation hearings; enforcement of confiscation orders; mutual legal assistance; terrorist financing; and civil forfeiture.

Civil Forfeiture

The course format was practically based with participants drafting orders and presenting applications in a courtroom setting. At the conclusion of the course, all prepared materials were given the participants on CD-ROM. Feedback from participants highlighted the benefit of the practical aspect of the workshop.

In December 2008 in Vanuatu, a series of workshops for stakeholders were held. The attendees were from casinos, money remitters, exchange houses, the legal profession, accountants, and trust and company service providers. The workshops covered, customer due diligence, monitoring, suspicious transaction reporting, and internal controls. The compliance with Vanuatu's Financial Transactions Reporting Act was central to the usefulness of the workshops for the stakeholders.

In 2007, the PALP hosted a national workshop on civil forfeiture for 19 prosecutors and law enforcement officials from Fiji. The objective of the workshop was to assist prosecutors and law enforcement in the use and application of the new civil forfeiture provisions. The workshop was funded by PALP and conducted jointly by the PALP and judges from the Fiji High Court. This has now resulted in a number of cases being brought before the High Court in Fiji for civil forfeiture.

Case Support

One of the key areas of the PALP's work is case support for jurisdictions in the region on high-profile money laundering cases. In 2008, the PALP provided case support to the Cook Islands, Palau, and the Marshall Islands.

PALP initiated multi-agency suspicious transaction report review teams hosted by the FIU's in Palau and the Marshall Islands. As a result of this multi-agency approach to reviewing FIU intelligence, several significant money laundering investigations have been initiated in Palau and the Marshall Islands. Although these investigations remain ongoing, one has already resulted in a 60-count indictment for money laundering and tax fraud violations.

The Year Ahead

PALP will continue to focus its technical assistance and training efforts on delivering targeted AML/CTF assistance through the work of senior mentors and trainers. PALP will direct its in-country assistance via mentoring and coaching as well as assistance with case development. In addition, PALP will deliver regional, sub-regional, and national training courses designed to give police investigators, customs officers, prosecutors, FIU staff, and regulators the knowledge and skills they need to identify, investigate, and prosecute money laundering and terrorist financing cases. PALP will grow in 2009 with the addition of another legal mentor to the team and greater use of our intermittent FIU and regulatory mentors.

United Nations Global Programme Against Money Laundering

The United Nations Global Programme against Money Laundering is one of the most experienced global providers of anti-money laundering (AML) training and technical assistance and, since 2001, training and technical assistance to combat the financing of terrorism (CTF). The UN Global Programme against Money Laundering, Proceeds of Crime, and the Financing of Terrorism (GPML), part of the UN Office on Drugs and Crime (UNODC), was established in 1997 to assist member states in complying with UN Conventions and other instruments that deal with money laundering and terrorist financing. These now include the UN Convention against Traffic in Narcotic Drugs and Psychotropic Substances (the 1988 Vienna Convention), the UN International Convention for the Suppression of the Financing of Terrorism (the 1999 Convention), the UN Convention against Transnational Organized Crime (the 2000 Palermo Convention), and the UN Convention against Corruption (the 2003 Merida Convention).

In March 2008, GPML's scope and objectives were widened to meet growing needs and demands of the international community for tailor-made assistance for implementing UN instruments and related international AML/CTF standards, and using AML/CTF systems as a tool to achieve improved financial transparency, integrity, and good governance. GPML has elaborated an ambitious program to make international action against the proceeds of crime and illegal financial flows more effective. This is done through a wide range of technical assistance measures and in close partnership with regional or multilateral organizations.

In September 2006, the UN General Assembly adopted the UN Global Counter-Terrorism Strategy. The plan of action contained in the strategy encourages UNODC to help countries comply with international norms and standards, and to enhance international cooperation in these areas. GPML is the focal point for AML policy and activities within the UN system and a key player in strengthening CTF efforts. GPML provides technical assistance and training in the development of related legislation, infrastructure, and skills, directly assisting member states in the detection, seizure, and confiscation of illicit proceeds. Since 2001, GPML's CTF technical assistance work has also received priority. As part of the implementation of the UN Global Counter-Terrorism Strategy, GPML is one of the lead entities in the UN Counter-Terrorism Implementation Task Force (CTITF) working group, an information-sharing and coordinating body aimed at developing policy recommendations in tackling the financing of terrorism. GPML now incorporates a focus on CTF in all its technical assistance work.

In 2008, GPML provided training and long-term assistance in the development of viable AML/CTF regimes to more than 50 countries. In September 2007, UNODC and the World Bank launched the Stolen Asset Recovery (StAR) Initiative, aimed at assisting developing countries to recover stolen assets that have been sent abroad by corrupt leaders. Given the close links between money laundering and corruption, and the fact that building an anti-money laundering system forms an integral part of good governance policy and asset recovery strategy, GPML participated in 2008 in several training events on confiscation of stolen assets.

The Mentoring Program

GPML's mentor program is a core part of GPML's technical assistance activities and serves as a model for other organizations' initiatives. The GPML mentoring program provides targeted on-the-job training that adapts international standards to specific local and national situations, rather than the traditional training seminar. The concept originated in response to repeated requests from member states for longer-term international assistance in this technically demanding and rapidly evolving field. GPML provides experienced prosecutors and law enforcement personnel who work side-by-side with

their counterparts in a target country for several months at a time on daily operational matters to help develop capacity. Some provide advice to governments on legislation and policy, while others focus on operating procedures, either with law enforcement or with issues relating to a country's financial intelligence unit (FIU). In many countries, GPML mentors are the only locally placed AML/CTF experts, and are heavily relied upon by local offices of donor countries and organizations for advice in the process of creation and delivery of other donor AML/CTF projects.

The GPML prosecutorial mentor based in Namibia's prosecutor general's office provides assistance for the development of asset forfeiture mechanisms in Botswana, Namibia, Zambia, and Zimbabwe. The mentor provided legal inputs to amend relevant legislation in each country, and continued to monitor the prosecutor placement program, an initiative aimed at placing prosecutors from the region for a certain period of time within the asset forfeiture unit of South Africa's national prosecuting authority.

In Eastern and Southern Africa, a law enforcement long-term consultant helped with the delivery of technical assistance, in particular a train-the-trainer certification program on financial investigations in Namibia and Tanzania. In collaboration with the U.S. Department of State and the World Bank, GPML extended the appointment of the regional mentor for Central Asia in Almaty, Kazakhstan, where the mentor focuses on legislative assistance and FIU development in Kazakhstan, Kyrgyzstan, Uzbekistan, Turkmenistan, and Tajikistan. The AML/CTF mentor in Hanoi, Vietnam, provided assistance to Vietnam, Laos, and Cambodia to establish comprehensive AML/CTF regimes, including the establishment and enhancement of FIUs. In October 2008, GPML assumed the coordination and administration role of the Pacific Anti-Money Laundering Program (PALP), which was established to provide AML/CTF advice, training, and technical assistance to support the establishment, development and implementation of AML/CTF regimes to 14 Pacific Island Forum jurisdictions that are not members of the FATF.

Mentoring and FIUs

GPML was among the first technical assistance providers to recognize the importance of countries creating financial intelligence capacity, and GPML mentors have worked extensively on the development and the implementation phases of FIUs in several countries in the Eastern Caribbean, Southern and Eastern Africa, the Pacific, Central Asia and in South East Asia. A major initiative that could have global implications for many FIUs is the development by the UNODC Information Technology Service (ITS), with substantive input from GPML, of an analytical and integrated database and intelligence analysis system for operational deployment in FIUs, called goAML (http://goaml.unodc.org). It is an IT solution for FIUs to manage their activities, particularly data collection, analysis, and dissemination. Version one of goAML is fully developed and has now been deployed in Namibia's and Kosovo's FIUs. It is likely that the next deployment will be to Tanzania's FIU. GoAML is also deployed at the Nigerian FIU and should soon be fully operational. In August 2008, goAML was evaluated by two of the world's leading FIUs, FINTRAC in Canada and AUSTRAC in Australia, on behalf of the Egmont Group. The positive outcome of the evaluation was reported to the IT Working Group of the Egmont Group in October 2008.

Computer-Based Training

Other highlights of GPML's work in 2008 included the ongoing development of its global computer-based training (CBT) initiative. The program provides 12 hours of interactive basic AML training, consisting of 13 modules for global delivery. The CBT training program has flexibility in terms of language, level of expertise, target audience, and theme. Computer-based training is particularly applicable in countries and regions with limited resources and law enforcement skills, as it can be used

for a sustained period of time. As an approach, CBT, which is translated into several languages, lends itself well to GPML's global technical assistance operations.

Delivery continued in particular with the deployment of additional CBT training classrooms in Rwanda (Police Criminal Investigations Department) and in the Russian Federation (Eurasian Group's International Training and Methodological Centre on Financial Monitoring), and a training center in Uganda (Police Headquarters). GPML also used its Amharic version of the CBT program and conducted a financial investigations training seminar, jointly with the Italian Guardia di Finanza, at the Police Academy of Ethiopia in October 2008. In 2008, GPML continued the development of additional CBT modules on asset forfeiture.

Other GPML Initiatives

GPML contributed to the delivery of mock trial training sessions in Latin America. This tailor-made activity was developed in response to repeated requests from member states for practical realistic AML training. It combines training and practical aspects of the judicial work into one capacity building exercise. Five mock trials were organized and delivered in 2008 in Brazil, Mexico, Peru, Uruguay, and Venezuela.

As part of the UNODC Rainbow Strategy, which aims to reduce the supply, trafficking, and consumption of opiates in Afghanistan and neighboring countries, GPML took the lead in a new initiative on "financial flows to and from Afghanistan linked to the illicit drug production and trafficking." An expert consultation meeting was held in November 2008 to comment on a draft background paper produced by a working group on the issue. The working group consists of representatives from the UNODC, International Monetary Fund (IMF), INTERPOL, Egmont Group, Eurasian Group, and the World Bank. The outcomes of this meeting were presented during the sixth Consultative Group Meeting of the Paris Pact held in Vienna in December 2008.

In 2008, GPML, in a collaborative effort with the IMF, finalized the revision of model provisions on AML/CTF and proceeds of crime for common law countries, encompassing worldwide AML/CTF standards and taking into account best legal practices. GPML continued to work closely with partners, including the U.S. Department of Justice, the U.S. Department of the Treasury's Office of Technical Assistance (OTA), the Organization for Security and Cooperation in Europe (OSCE), the Commonwealth Secretariat, the IMF, and the World Bank, to deliver CTF training, particularly in the regions of Central Asia, Southern Europe, South Asia and the Pacific, and Africa.

GPML administers the Anti-Money Laundering International Database (AMLID) on the International Money Laundering Information Network (IMoLIN), an online, password-restricted, analytical database of national AML/CTF legislation that is available only to public officials. The database now contains legislation from some 180 jurisdictions.

GPML also maintains an online AML/CTF legal library and issues a Central Asia Newsletter monthly in English and quarterly in Russian. IMoLIN (www.imolin.org) is a practical tool in daily use by government officials, law enforcement, and lawyers. In 2007, GPML launched the French language version of IMoLIN and continued its second round of legal analysis using a revised AMLID questionnaire. The updated AMLID questionnaire reflects new money laundering trends and standards, and takes provisions related to terrorist financing and other new developments into account, including the revised FATF recommendations. In 2008, 15 new questionnaires were uploaded to the database, raising the total of revised AMLID questionnaires in the database under the second round of legal analysis to more than 70.

Law Enforcement Cases

Lloyds of London Violates IEEPA

Lloyds TSB Bank, a United Kingdom corporation headquartered in London, has agreed to forfeit $350 million to the United States and to the New York County District Attorney's Office in connection with violations of the International Emergency Economic Powers Act (IEEPA). The violations relate to transactions Lloyds illegally conducted on behalf of customers from Iran, Sudan and other countries sanctioned in programs administered by the Office of Foreign Assets Controls.

A criminal information was filed in the U.S. District Court for the District of Columbia charging Lloyds with one count of violating the IEEPA. Lloyds waived indictment, agreed to the filing of the information, and has accepted and acknowledged responsibility for its criminal conduct. Lloyds agreed to forfeit the funds as part of deferred prosecution agreements with the Department of Justice and the New York County District Attorney's Office.

Under the IEEPA, it is a crime to willfully violate, or attempt to violate, any regulation issued under the act, including the Iranian Transactions Regulations, which prohibit exportation of services from the United States to Iran, and the Sudanese Sanctions Regulations, which prohibit exportation of services from the United States to Sudan.

According to court documents, beginning as early as 1995 and continuing until January 2007, Lloyds, in both the United Kingdom and Dubai, falsified outgoing U.S. wire transfers that involved countries or persons on U.S. sanctions lists. Specifically, according to court documents, Lloyds deliberately removed material information—such as customer names, bank names and addresses—from payment messages so that the wire transfers would pass undetected through filters at U.S. financial institutions. This process of "repairing" or "stripping," as Lloyds commonly referred to it, allowed more than $350 million in transactions to be processed by U.S. correspondent banks used by Lloyds that might have otherwise been blocked or rejected due to sanctions regulations or for internal bank policy reasons. According to court documents, the criminal conduct by Lloyds was designed to evade, and to assist its customers in evading, U.S. economic sanctions imposed against Iran, Sudan and other countries.

"For more than 12 years, Lloyds facilitated the anonymous movement of hundreds of millions of dollars from U.S.-sanctioned nations through our financial system," said Acting Assistant Attorney General Matthew Friedrich. "More than $350 million moved from places such as Iran through locations around the world because Lloyds stripped identifying information from international wire transfers that would have raised a red flag at U.S. financial institutions and caused such payments to be scrutinized. The Department will continue to use criminal enforcement measures against the knowing and intentional evasion of U.S. sanctions laws, particularly where such conduct has the potential to finance terrorist activities."

The bank's forfeiture of $175 million to the United States and $175 million to New York County will settle forfeiture claims by the Department of Justice and the state of New York related to the misconduct. In light of the bank's remedial actions to date and its willingness to acknowledge responsibility for its actions, the Department will recommend the dismissal of the information in two years, provided Lloyds fully cooperates with, and abides by, the terms of the agreement.

The case was prosecuted by the Department of Justice Criminal Division's Asset Forfeiture and Money Laundering Section and was investigated by the IRS-Criminal Investigation's Washington Field Division.

Holy Land Foundation Revisited

On November 24, 2008, in the Northern District of Texas, all defendants in United States v. Holy Land Foundation were found guilty by a jury of all counts charged. On November 12, 2008, the jury began deliberating. The defense rested its case on November 6, 2008, and closing statements began on Monday, November 10, 2008. Holy Land Foundation ("HLF") was a Hamas front organization that received start up assistance from Mousa Abu Marzook—a leader of Hamas and a specially designated terrorist—and raised millions of dollars for Hamas over a thirteen-year period. The new trial results from a mistrial declared on October 22, 2007, in the Northern District of Texas, when a jury found defendant Mohammed El-Mezain not guilty as to most charges, but failed to reach a verdict on a material support count against him, and deadlocked on the remaining counts against the other defendants. All other defendants at trial—Shukri Abu Baker, Ghassan Elashi, Mufid Abdulqader, and Abdulraham Odeh—and all counts resulted in a mistrial. The case was re-assigned for retrial in 2008. HLF received start up assistance from Mousa Abu Marzook, a leader of Hamas. It was the largest Muslim charity in the United States until it was declared a Specially Designated Terrorist Organization in 2001 and shut down. HLF raised millions of dollars for Hamas over a 13-year period.

Hawala, Money Laundering and Terrorism Financing

On November 4, 2008, in the District of Maryland, Saifullah Anjum Ranjha, a Pakistani national residing in Washington, D.C. and Maryland, was sentenced to 110 months in prison, followed by three years of supervised release, for conspiring to launder money and for concealing terrorist financing. The judge also signed a preliminary order forfeiting $2,208,000 of Ranjha's assets.

Ranjha was born in Pakistan and became a lawful permanent resident of the United States in September 1997. He operated a money remitter business in the District of Columbia known as Hamza, Inc. During the U.S. Immigration and Customs Enforcement (ICE) led investigation, a cooperating witness, acting at the direction of law enforcement, presented himself to Ranjaha and his associates as someone involved in large scale international drug trafficking, international smuggling of counterfeit cigarettes and weapons. He also represented that he was providing assistance and financing to members of al Qaeda and its affiliated organizations and their operatives. From October 2003 to September 19, 2007, the cooperating witness gave Ranjha and his associates a total of $2,208,000 in government funds to transfer the monies abroad through the hawala informal money transfer system, bypassing conventional banking systems and regulations.

The cooperating witness represented that the monies were the proceeds of his purported illegal activities. There were a total of 21 hawala transactions in amounts ranging from $13,000 to $300,000. Most of the monies were turned over to Ranjha in locations in Maryland. On a few occasions the cooperating witness met Ranjha and other co-conspirators at Hamza, Inc. to provide monies for a particular hawala transfer. Ranjha arranged with his associates for the equivalent amount of monies, minus commissions, to be delivered to the cooperating witness, his third party designee, or a designated bank account in Canada, England, Spain, Pakistan, Japan and Australia. Ranjha kept a commission of approximately five percent of the amount of currency transferred. Other conspirators involved in a particular transaction retained an additional commission of between three to five percent of the transaction amount. All the funds transferred abroad were picked up by cooperating individuals and returned to the Government.

Other agencies involved in the investigation included, the Federal Bureau of Investigation and the Internal Revenue Service—Criminal Division. International law enforcement partners included the Spanish National Police, Australian Federal Police, London Metropolitan Police, and Royal Canadian Mounted Police.

NGO Support of a Terror Organization

On August 25, 2008, in the Southern District of Florida, Richard David Hupper was sentenced to 46 months in prison and a $15,000 fine. He had pled guilty on May 21, 2008, to one count of providing material support to Hamas, in violation of 18 U.S.C. § 2339B.

Between December 2004 and September 2006, Hupper, a United States citizen, traveled on numerous occasions to the Middle East. He met and worked with individuals in the International Solidarity Movement (ISM), a pro-Palestinian nongovernmental organization (NGO), and gradually became interested in assisting Hamas. Through his contacts with ISM, Hupper became friendly with a major figure in the ISM and a suspected Hamas member. On several occasions during an approximate two year period of time, Hupper provided money, both in person and via Western Union wire transfer, with knowledge that the funds he gave were going directly to Hamas. These funds were to be used by Hamas in a variety of ways including assisting the families of Israeli-imprisoned Hamas members. Hupper also procured a fraudulent passport using an alias after the government restricted his travel to the Middle East. He was earlier arrested and prosecuted for identity theft. After his arrest on the identity theft charges, Hupper was interviewed and admitted to the illegal conduct to which he later pled.

"Bust-Out" Scheme

In August 2008, in the Central District of California, Reza Bahram Tabatabai was sentenced to 87 months in federal prison and ordered to pay $2,235,801 in restitution.

Tabatabai was found guilty of conspiracy, seven counts of interstate transportation of fraudulently obtained property, six counts of mail fraud, eight counts of wire fraud, conspiracy to commit money laundering and 33 counts of money laundering in connection with a series of "bust-out" schemes in which several companies were taken over and their credit lines were exhausted.

Tabatabai, with the help of several others, purchased established businesses so they could make large purchases of goods using the companies' existing lines of credit. The goods sold to the companies were re-sold at discounted prices to quickly generate profits for the participants in the scheme. Although some payments were made in order to secure larger lines of credit, lenders to the four companies lost more than $8 million. The evidence at trial showed that Tabatabai and his co-conspirators engaged in a series of complex monetary transactions to both conceal and promote the fraudulent scheme. Tabatabai controlled numerous bank accounts, held in the names of numerous businesses, in which he concealed the proceeds of the fraudulent conduct.

Previously, in October 1999, Tabatabai was charged in a Superseding Information with one count of conspiracy, in violation of 18 U.S.C. § 371, and one count of providing material support to a designated foreign terrorist organization, the Mujahedin-e-Khalq (MEK), in violation of 18 U.S.C. § 2339B. Tabatabai pled guilty to the charges and was sentenced to 24 months in prison.

Sentencing Hearings Held in CARE International Case

Defendants Emadeddin Muntasser, Muhamed Mubayyid, and Samir al-Monla were charged in a March 8, 2007 superseding indictment with a scheme to defraud various United States agencies of information relating to a Massachusetts charity known as Care International. In January 2008 the defendants were found guilty of charges including a Scheme to Conceal Material Facts and Aiding and Abetting, in violation of 18 U.S.C. §§ 1001(a)(1) and 2; Conspiracy to Defraud the United States, in violation of 18 U.S.C. § 371; and Obstructing and Impeding the Internal Revenue Service, in violation of 26 U.S.C. § 7212(a). Mubayyid was found guilty of three additional counts of Filing a False Tax Return, in violation of 26 U.S.C. § 7206(1), and Muntasser was found guilty of one count of False

Statements to the FBI, in violation of 18 U.S.C. § 1001(a)(2). On June 3, 2008, the District Judge dismissed, post verdict, a number of charges against Mubayyid and Muntasser under Rule 29 of the Federal Rules of Criminal Procedure. Defendant Samir al-Monla was acquitted on all charges. The United States Attorney's Office has filed a notice of appeal.

On July 18, 2008, in the District of Massachusetts, Mubayyid was sentenced to 11 months in prison followed by 3 years of supervised release. Mubayyid was also ordered to pay a $1,000 fine and a $500.00 special assessment. On July 17, 2008, Muntasser was sentenced to 12 months in prison followed by 3 years of supervised release. Muntasser was ordered to pay a $10,000 fine and a $100.00 special assessment.

Muntasser formed Care International in 1993, shortly after another organization with which he was associated, the Al-Kifah Refugee Center, was publicly implicated in the first World Trade Center Bombing. Thereafter, Muntasser, Mubayyid, and Al-Monla filed a number of false documents with the Internal Revenue Service, concealing the fact that Care International was an outgrowth of Al Kifah and was continuing its support of mujaheddin and violent jihad overseas. Al-Monla served as the president of Care from 1996-1998 while Mubayyid is the former treasurer of the organization. After the September 11, 2001 terrorist attacks, the defendants made false statements to the FBI about Care International's operations, and Muntasser falsely denied on his U.S. naturalization application that he was affiliated with any organization or that he had traveled to Afghanistan.

Money Laundering and Harboring Illegal Aliens

In a U.S. Immigration and Customs Enforcement (ICE) led investigation in Greenbelt, Md., Juan Faustino Solano of Kensington, Md., was sentenced to 15 months in prison, for money laundering and conspiracy to commit alien harboring in connection with the operation of the El Pollo Rico restaurant in Wheaton, Maryland. Juan's sister, Consuelo Solano, 69, of Arlington, Virginia, was sentenced to two months in prison for money laundering. Both Juan Solano and Consuelo Solano were ordered to forfeit $7.2 million derived from the illegal activities, including 13 bank and investor accounts, a life insurance policy, eight properties in Maryland, three vehicles, collectible coins, and jewelry. Moreover, as part of this amount, Consuelo Solano has to forfeit over $2.1 million in cash found in her home.

Juan Solano conspired with others to employ illegal aliens and undocumented workers at the restaurant from January 1999 to July 2007, paying them in cash and housing them in multiple residences owned by Solano and his co-conspirators in Maryland. To further the conspiracy, Solano did not prepare or maintain Employment Eligibility Verification Forms for those employees, which establish the eligibility of an individual to be employed in the United States legally.

In addition, Consuelo and Juan Solano admitted that they conspired to conceal the proceeds from the illegal employment of aliens. They deposited more than $7 million from the operation of the restaurant into the El Pollo Rico business account from 2002 to 2007. Transfers were made from the El Pollo Rico business account to business and personal accounts. As a result of their roles in alien harboring and in conducting these deposits, transfers, and purchases involving the proceeds of alien harboring, both Juan and Consuelo Solano will receive enhanced sentences for managing and organizing criminal activity.

Major Money Laundering Countries

Every year, U.S. officials from agencies with anti-money laundering responsibilities meet to assess the money laundering situations in 200 jurisdictions. The review includes an assessment of the significance of financial transactions in the country's financial institutions involving proceeds of

serious crime, steps taken or not taken to address financial crime and money laundering, each jurisdiction's vulnerability to money laundering, the conformance of its laws and policies to international standards, the effectiveness with which the government has acted, and the government's political will to take needed actions.

The 2009 INCSR identified money laundering priority jurisdictions and countries using a classification system that consists of three different categories: Jurisdictions of Primary Concern, Jurisdictions of Concern, and Other Jurisdictions Monitored.

"Jurisdictions of Primary Concern" are those that are identified, pursuant to INCSR reporting requirements, as "major money laundering countries." A major money laundering country is defined by statute as one "whose financial institutions engage in currency transactions involving significant amounts of proceeds from international narcotics trafficking." However, the complex nature of money laundering transactions today makes it difficult in many cases to distinguish the proceeds of narcotics trafficking from the proceeds of other serious crime. Moreover, financial institutions engaged in transactions that involve significant amounts of proceeds from other serious crimes are vulnerable to narcotics-related money laundering. The category "Jurisdiction of Primary Concern" recognizes this relationship by including all countries and other jurisdictions whose financial institutions engage in transactions involving significant amounts of proceeds from all serious crimes. Thus, the focus in considering whether a country or jurisdiction should be included in this category is on the significance of the amount of proceeds laundered, not of the anti-money laundering measures taken. This is a different approach taken than that of the Financial Action Task Force's Non-Cooperative Countries and Territories (NCCT) exercise, which focuses on a jurisdiction's compliance with stated criteria regarding its legal and regulatory framework, international cooperation, and resource allocations.

All other countries and jurisdictions evaluated in the INCSR are separated into the two remaining groups, "Jurisdictions of Concern" and "Other Jurisdictions Monitored," on the basis of several factors that may include: (1) whether the country's financial institutions engage in transactions involving significant amounts of proceeds from serious crimes; (2) the extent to which the jurisdiction is or remains vulnerable to money laundering, notwithstanding its money laundering countermeasures, if any (an illustrative list of factors that may indicate vulnerability is provided below); (3) the nature and extent of the money laundering situation in each jurisdiction (e.g., whether it involves drugs or other contraband); (4) the ways in which the U.S. Government (USG) regards the situation as having international ramifications; (5) the situation's impact on U.S. interests; (6) whether the jurisdiction has taken appropriate legislative actions to address specific problems; (7) whether there is a lack of licensing and oversight of offshore financial centers and businesses; (8) whether the jurisdiction's laws are being effectively implemented; and (9) where U.S. interests are involved, the degree of cooperation between the foreign government and the USG. Additionally, given concerns about the increasing interrelationship between inadequate money laundering legislation and terrorist financing, terrorist financing is an additional factor considered in making a determination as to whether a country should be considered a "Jurisdiction of Concern" or an "Other Jurisdiction Monitored." A government (e.g., the United States or the United Kingdom) can have comprehensive anti-money laundering laws on its books and conduct aggressive anti-money laundering enforcement efforts but still be classified a "Primary Concern" jurisdiction. In some cases, this classification may simply or largely be a function of the size of the jurisdiction's economy. In such jurisdictions, quick, continuous and effective anti-money laundering efforts by the government are critical. While the actual money laundering problem in jurisdictions classified as "Jurisdictions of Concern" is not as acute, they too must undertake efforts to develop or enhance their anti-money laundering regimes. Finally, while jurisdictions in the "Other Jurisdictions Monitored" category do not pose an immediate concern, it is nevertheless important to monitor their money laundering situations because, under certain circumstances, virtually any jurisdiction of any size can develop into a significant money laundering center.

Vulnerability Factors

The current ability of money launderers to penetrate virtually any financial system makes every jurisdiction a potential money laundering center. There is no precise measure of vulnerability for any financial system, and not every vulnerable financial system will, in fact, be host to large volumes of laundered proceeds. A checklist of what drug money managers reportedly look for, however, provides a basic guide. The checklist includes:

- Failure to criminalize money laundering for all serious crimes or limiting the offense to narrow predicates.
- Rigid bank secrecy rules that obstruct law enforcement investigations or that prohibit or inhibit large value and/or suspicious or unusual transaction reporting by both banks and nonbank financial institutions.
- Lack of or inadequate "know your customer" requirements to open accounts or conduct financial transactions, including the permitted use of anonymous, nominee, numbered or trustee accounts.
- No requirement to disclose the beneficial owner of an account or the true beneficiary of a transaction.
- Lack of effective monitoring of cross-border currency movements.
- No reporting requirements for large cash transactions.
- No requirement to maintain financial records over a specific period of time.
- No mandatory requirement to report suspicious transactions or a pattern of inconsistent reporting under a voluntary system and a lack of uniform guidelines for identifying suspicious transactions.
- Use of bearer monetary instruments.
- Well-established nonbank financial systems, especially where regulation, supervision, and monitoring are absent or lax.
- Patterns of evasion of exchange controls by legitimate businesses.
- Ease of incorporation, in particular where ownership can be held through nominees or bearer shares, or where off-the-shelf corporations can be acquired.
- No central reporting unit for receiving, analyzing, and disseminating to the competent authorities information on large value, suspicious or unusual financial transactions that might identify possible money laundering activity.
- Lack of or weak bank regulatory controls, or failure to adopt or adhere to Basel Committee's "Core Principles for Effective Banking Supervision," especially in jurisdictions where the monetary or bank supervisory authority is understaffed, under-skilled or uncommitted.
- Well-established offshore financial centers or tax-haven banking systems, especially jurisdictions where such banks and accounts can be readily established with minimal background investigations.
- Extensive foreign banking operations, especially where there is significant wire transfer activity or multiple branches of foreign banks, or limited audit authority over foreign-owned banks or institutions.

- Jurisdictions where charitable organizations or alternate remittance systems, because of their unregulated and unsupervised nature, are used as avenues for money laundering or terrorist financing.
- Limited asset seizure or confiscation authority.
- Limited narcotics, money laundering, and financial crime enforcement, and lack of trained investigators or regulators.
- Jurisdictions with free trade zones where there is little government presence or other supervisory authority.
- Patterns of official corruption or a laissez-faire attitude toward business and banking communities.
- Jurisdictions where the U.S. dollar is readily accepted, especially jurisdictions where banks and other financial institutions allow dollar deposits.
- Well-established access to international bullion trading centers in New York, Istanbul, Zurich, Dubai, and Mumbai.
- Jurisdictions where there is significant trade in or export of gold, diamonds, and other gems.
- Jurisdictions with large parallel or black market economies.
- Limited or no ability to share financial information with foreign law enforcement authorities.

Changes in INCSR Priorities for 2008

Countries moving to the "Jurisdictions of Primary Concern" category from the "Jurisdictions of Concern" category: **Bolivia, Guinea-Bissau, and Zimbabwe**.

Countries moving to the "Jurisdictions of Concern" category from the "Other Jurisdictions Monitored" category: **Azerbaijan and Trinidad and Tobago**.

Country moving to "Other Jurisdictions Monitored" category from the "Jurisdictions of Concern" category: **Dominica**

In the Country/Jurisdiction Table on the following page, "major money laundering countries" that are in the "Jurisdictions of Primary Concern" category are identified for purposes of INCSR statutory reporting requirements. Identification as a "major money laundering country" is based on whether the country or jurisdiction's financial institutions engage in transactions involving significant amounts of proceeds from serious crime. It is not based on an assessment of the country or jurisdiction's legal framework to combat money laundering; its role in the terrorist financing problem; or the degree of its cooperation in the international fight against money laundering, including terrorist financing. These factors, however, are included among the vulnerability factors when deciding whether to place a country or jurisdiction in the "Jurisdictions of Concern" or "Other Jurisdictions Monitored" category.

Note: Country reports are provided for only those countries and jurisdictions listed in the "Primary Jurisdictions of Concern" and "Jurisdictions of Concern" categories.

Country/Jurisdiction Table

Countries/Jurisdictions of Primary Concern

Afghanistan
Antigua and Barbuda
Australia
Austria
Bahamas
Belize
Bolivia
Brazil
Burma
Cambodia
Canada
Cayman Islands
China, People Rep
Colombia
Costa Rica
Cyprus
Dominican Republic
France
Germany
Greece
Guatemala
Guernsey
Guinea-Bissau
Haiti
Hong Kong
India
Indonesia
Iran
Isle of Man
Israel
Italy
Japan
Jersey
Kenya
Latvia
Lebanon
Liechtenstein
Luxembourg
Macau
Mexico
Netherlands
Nigeria
Pakistan
Panama
Paraguay
Philippines
Russia
Singapore
Spain
Switzerland
Taiwan
Thailand
Turkey
Ukraine
United Arab Emirates
United Kingdom
United States
Uruguay
Venezuela
Zimbabwe

Countries/Jurisdictions of Concern

Albania
Algeria
Angola
Argentina
Aruba
Azerbaijan
Bahrain
Bangladesh
Barbados
Belarus
Belgium
Bosnia and Herzegovina
British Virgin Islands
Bulgaria
Chile
Comoros
Cook Islands
Cote d'Ivoire
Czech Rep
Ecuador
Egypt
El Salvador
Ghana
Gibraltar
Grenada
Guyana
Honduras
Hungary
Iraq
Ireland
Jamaica
Jordan
Korea, North
Korea, South
Kuwait
Laos
Malaysia
Moldova
Monaco
Morocco
Netherlands Antilles
Nicaragua
Palau
Peru
Poland
Portugal
Qatar
Romania
Samoa
Saudi Arabia
Senegal
Serbia
Seychelles
Sierra Leone
Slovakia
South Africa
St. Kitts & Nevis
St. Lucia
St. Vincent
Suriname
Syria
Tanzania
Trinidad and Tobago
Turks and Caicos
Uzbekistan
Vanuatu
Vietnam
Yemen

Other Countries/Jurisdictions Monitored

Andorra
Anguilla
Armenia
Benin
Bermuda
Botswana
Brunei
Burkina Faso
Burundi
Cameroon
Cape Verde
Central African Republic
Chad
Congo, Dem Rep of
Congo, Rep of
Croatia
Cuba
Denmark
Djibouti
Dominica
East Timor
Equatorial Guinea
Eritrea
Estonia
Ethiopia
Fiji
Finland
Gabon
Gambia
Georgia
Guinea
Iceland
Kazakhstan
Kosovo
Kyrgyz Republic
Lesotho
Liberia
Libya
Lithuania
Macedonia
Madagascar
Malawi
Maldives
Mali
Malta
Marshall Islands
Mauritania
Mauritius
Micronesia FS
Mongolia
Montenegro
Montserrat
Mozambique
Namibia
Nauru
Nepal
New Zealand
Niger
Niue
Norway
Oman
Papua New Guinea
Rwanda
San Marino
Sao Tome & Principe
Slovenia
Solomon Islands
Sri Lanka
Swaziland
Sweden
Tajikistan
Togo
Tonga
Tunisia
Turkmenistan
Uganda
Zambia

Introduction to Comparative Table

The comparative table that follows the Glossary of Terms below identifies the broad range of actions, effective as of December 31, 2008, that jurisdictions have, or have not, taken to combat money laundering. This reference table provides a comparison of elements that includes legislative activity and other identifying characteristics that can have a relationship to a jurisdiction's money laundering vulnerability.

Glossary of Terms

1. "Criminalized Drug Money Laundering": The jurisdiction has enacted laws criminalizing the offense of money laundering related to drug trafficking.
2. "Criminalized Beyond Drugs": The jurisdiction has extended anti-money laundering statutes and regulations to include nondrug-related money laundering.
3. "Record Large Transactions": By law or regulation, banks are required to maintain records of large transactions in currency or other monetary instruments.
4. "Maintain Records Over Time": By law or regulation, banks are required to keep records, especially of large or unusual transactions, for a specified period of time, e.g., five years.
5. "Report Suspicious Transactions": By law or regulation, banks are required to record and report suspicious or unusual transactions to designated authorities. On the Comparative Table the letter "M" signifies mandatory reporting; "P" signifies permissible reporting.
6. "Financial Intelligence Unit": The jurisdiction has established an operative central, national agency responsible for receiving (and, as permitted, requesting), analyzing, and disseminating to the competent authorities disclosures of financial information concerning suspected proceeds of crime, or required by national legislation or regulation, in order to counter money laundering. These reflect those jurisdictions that are members of the Egmont Group.
7. "System for Identifying and Forfeiting Assets": The jurisdiction has enacted laws authorizing the tracing, freezing, seizure, and forfeiture of assets identified as relating to or generated by money laundering activities.
8. "Arrangements for Asset Sharing": By law, regulation or bilateral agreement, the jurisdiction permits sharing of seized assets with third party jurisdictions that assisted in the conduct of the underlying investigation.
9. "Cooperates w/International Law Enforcement": By law or regulation, banks are permitted/required to cooperate with authorized investigations involving or initiated by third party jurisdictions, including sharing of records or other financial data.
10. "International Transportation of Currency": By law or regulation, the jurisdiction, in cooperation with banks, controls or monitors the flow of currency and monetary instruments crossing its borders. Of critical weight here is the presence or absence of wire transfer regulations and use of reports completed by each person transiting the jurisdiction and reports of monetary instrument transmitters.
11. "Mutual Legal Assistance": By law or through treaty, the jurisdiction has agreed to provide and receive mutual legal assistance, including the sharing of records and data.
12. "Nonbank Financial Institutions": By law or regulation, the jurisdiction requires nonbank financial institutions to meet the same customer identification standards and adhere to the same reporting requirements that it imposes on banks.

13. “Disclosure Protection Safe Harbor”: By law, the jurisdiction provides a “safe harbor” defense to banks or other financial institutions and their employees who provide otherwise confidential banking data to authorities in pursuit of authorized investigations.
14. “States Parties to 1988 UN Drug Convention”: States parties to the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, or a territorial entity to which the application of the Convention has been extended by a party to the Convention.
15. “Criminalized the Financing of Terrorism”: The jurisdiction has criminalized the provision of material support to terrorists and/or terrorist organizations.
16. “States Parties to the UN International Convention for the Suppression of the Financing of Terrorism”: States parties to the International Convention for the Suppression of the Financing of Terrorism, or a territorial entity to which the application of the Convention has been extended by a party to the Convention.

Comparative Table

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions (NMP)	Egmont Financial Intelligence Units	System for Identifying/Forfeiting Assets	Arrangements for Asset Sharing	Cooperates w/International Law Enf.	International Transportation of Currency	Mutual Legal Assistance	Non-Bank Financial Institutions	Disclosure Protection "Safe Harbor"	Criminalized Financing of Terrorism	States Party to 1988 UN Convention	Intl. Terrorism Financing Convention
Government/Jurisdiction																
Afghanistan	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Albania	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Algeria	Y	Y	N	Y	M	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Andorra	Y	Y	Y	Y	M	Y	Y	N	Y	N	Y	Y	Y	N	Y	Y
Angola	Y	N	N	N	N	N	N	N	N	N	Y	N	N	N	Y	N
Anguilla[1]	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N
Antigua & Barbuda	Y	Y	N	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Argentina	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Armenia	Y	Y	N	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Aruba	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Australia	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Austria	Y	Y	N	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Azerbaijan	Y	N	N	Y	N	N	N	N	N	Y	Y	N	N	Y	Y	Y
Bahamas	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Bahrain	Y	Y	N	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Bangladesh	Y	Y	N	Y	M	N	N	N	N	Y	Y	N	N	Y	Y	Y
Barbados	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Belarus	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Belgium	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Belize	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Benin	Y	Y	N	Y	M	N	Y	N	Y	Y	N	N	Y	N	Y	Y

[1] The UK extended its application of the 1988 Convention and the UK Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Montserrat, the Turks and Caicos, Isle of Man, Bailiwick of Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions (NMP)	Egmont Financial Intelligence Units	System for Identifying/Forfeiting Assets	Arrangements for Asset Sharing	Cooperates w/International Law Enf.	International Transportation of Currency	Mutual Legal Assistance	Non-Bank Financial Institutions	Disclosure Protection "Safe Harbor"	Criminalized Financing of Terrorism	States Party to 1988 UN Convention	Intl. Terrorism Financing Convention
Bermuda[1]	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Bolivia[2]	Y	Y	Y	Y	M	N	Y	N	N	N	Y	N	Y	N	Y	Y
Bosnia & Herzegovina	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Botswana	Y	Y	Y	Y	M	N	Y	Y	Y	Y	Y	N	Y	N	Y	Y
Brazil	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
British Virgin Islands[1]	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Brunei Darussalam	Y	Y	N	Y	M	N	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Bulgaria	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Burkina Faso	N	N	Y	Y	M	N	N	N	N	N	N	N	N	N	Y	Y
Burma	Y	Y	Y	Y	M	N	Y	N	Y	N	Y	Y	Y	N	Y	Y
Burundi	N	N	N	Y	N	N	Y	N	Y	Y	N	N	N	N	Y	N
Cambodia	Y	N	Y	Y	M	N	N	N	Y	Y	N	N	N	Y	Y	Y
Cameroon	Y	Y	Y	Y	M	N	Y	N	N	N	N	N	N	N	Y	Y
Canada	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Cape Verde	Y	Y		Y	M	N	Y	N			Y			N	Y	Y
Cayman Islands[1]	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Chad	Y	Y	Y	Y	M	N	Y	N	N	Y	N	N	N	N	Y	N
Chile	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
China (PRC)	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	N	Y	Y	Y
Colombia	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Comoros	Y	Y	N	Y	M	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Congo (Dem. Republic)	Y	Y	Y	Y	M	N	Y	N	N	N	N	Y	Y	Y	Y	Y

[1] The UK extended its application of the 1988 Convention and the UK Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Montserrat, the Turks and Caicos, Isle of Man, Bailiwick of Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

[2] Bolivia's FIU was suspended from membership in the Egmont Group on July 31, 2007

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions (NMP)	Egmont Financial Intelligence Units	System for Identifying/Forfeiting Assets	Arrangements for Asset Sharing	Cooperates w/International Law Enf.	International Transportation of Currency	Mutual Legal Assistance	Non-Bank Financial Institutions	Disclosure Protection "Safe Harbor"	Criminalized Financing of Terrorism	States Party to 1988 UN Convention	Intl. Terrorism Financing Convention
Congo (Republic)	Y	Y	Y	Y	M	N	N	N	N	N	Y	Y	Y	Y	Y	Y
Cook Islands	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Costa Rica	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y
Cote D'Ivoire	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	N	Y	Y
Croatia	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Cuba	Y	Y	N	N	P	N	Y	N	N	Y	N	N	N	Y	Y	Y
Cyprus (ROC)	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Cyprus ("TRNC")	Y	Y	Y	Y	M	N	N	N	N	Y	N	N			NA	NA
Czech Republic	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Denmark	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Djibouti	Y	Y	Y	Y	M	N	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Dominica	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Dominican Republic	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
East Timor	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Ecuador	Y	Y	Y	Y	M	N	Y	Y	N	Y	Y	Y	N	N	Y	Y
Egypt	Y	Y	N	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
El Salvador	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Equatorial Guinea	Y	Y	Y	Y	M	N	N	N	N	N	N	N	N	N	N	Y
Eritrea	N	N	Y	Y	N	N	N	N	Y	Y	N	N	N	N	Y	N
Estonia	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Ethiopia	Y	Y	Y	Y	M	N	N	N	N	N	N	N	N	N	Y	N
Fiji	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Finland	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
France	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Gabon	N	N	Y	Y	M	N	N	N	N	N	N	Y	N	N	Y	Y
Gambia	Y	Y	N	Y	M	N	Y	N	N	N	N	N	Y	N	Y	N

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions (NMP)	Egmont Financial Intelligence Units	System for Identifying/Forfeiting Assets	Arrangements for Asset Sharing	Cooperates w/International Law Enf.	International Transportation of Currency	Mutual Legal Assistance	Non-Bank Financial Institutions	Disclosure Protection "Safe Harbor"	Criminalized Financing of Terrorism	States Party to 1988 UN Convention	Intl. Terrorism Financing Convention
Georgia	Y	Y	Y	Y	M	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Germany	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Ghana	Y	Y	N	Y	M	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Gibraltar[1]	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	N	N
Greece	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Grenada	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Guatemala	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Guernsey[1]	Y	Y	N	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N
Guinea	Y	N	N	N	N	N	N	N	N	Y	N	N	N	N	Y	Y
Guinea-Bissau	Y	Y	Y	Y	M	N	N	N	N	N	Y	Y	Y	Y	Y	Y
Guyana	Y	Y	N	Y	M	N	Y	N	N	Y	Y	N	Y	N	Y	Y
Haiti	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	N	Y	N
Honduras	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Hong Kong[2]	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Hungary	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Iceland	Y	Y	Y	Y	M	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y
India	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Indonesia	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Iran	N	N	N	Y	M	N	N	N	N	N	N	N	N	N	Y	N
Iraq	Y	Y	Y	Y	M	N	Y	N	N	Y	N	Y	Y	Y	Y	N
Ireland	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Isle of Man[1]	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N

[1] The UK extended its application of the 1988 Convention and the UK Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Montserrat, the Turks and Caicos, Isle of Man, Bailiwick of Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

[2] The People's Republic of China extended the UN Financing of Terrorism Convention to the Special Administrative Regions of Hong Kong and Macau.

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions (NMP)	Egmont Financial Intelligence Units	System for Identifying/Forfeiting Assets	Arrangements for Asset Sharing	Cooperates w/International Law Enf.	International Transportation of Currency	Mutual Legal Assistance	Non-Bank Financial Institutions	Disclosure Protection "Safe Harbor"	Criminalized Financing of Terrorism	States Party to 1988 UN Convention	Intl. Terrorism Financing Convention
Israel	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Italy	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Jamaica	Y	Y	Y	Y	M	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Japan	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Jersey[1]	Y	Y	N	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N
Jordan	Y	Y	N	Y	M	N	Y	Y	N	N	Y	Y	Y	Y	Y	Y
Kazakhstan	Y	N	N	Y	P	N	N	N	N	Y	Y	N	N	Y	Y	Y
Kenya	Y	N	Y	Y	P	N	N	N	Y	Y	Y	N	N	N	Y	Y
Korea (DPRK)	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N
Korea (Republic of)	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y
Kosovo	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	Y	NA	NA
Kuwait	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	N	Y	N
Kyrgyzstan	Y	N	Y	Y	M	N	Y	N	N	N	Y	Y	Y	N	Y	Y
Laos	Y	Y	N	N	M	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y
Latvia	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Lebanon	Y	Y	Y	Y	M	Y	Y	N	Y	N	Y	Y	Y	Y	Y	N
Lesotho	N	N	Y	Y	M	N	N	N	Y	N	Y	N	Y	N	Y	Y
Liberia	N	Y	N	Y	P	N	N	N	Y	Y	N	N	N	N	Y	Y
Libya	Y	Y	N	Y	M	N	N	N	N	N	N	Y	Y	N	Y	Y
Liechtenstein	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Lithuania	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Luxembourg	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y

[1] The UK extended its application of the 1988 Convention and the UK Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Montserrat, the Turks and Caicos, Isle of Man, Bailiwick of Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions (NMP)	Egmont Financial Intelligence Units	System for Identifying/Forfeiting Assets	Arrangements for Asset Sharing	Cooperates w/International Law Enf.	International Transportation of Currency	Mutual Legal Assistance	Non-Bank Financial Institutions	Disclosure Protection "Safe Harbor"	Criminalized Financing of Terrorism	States Party to 1988 UN Convention	Intl. Terrorism Financing Convention
Macau[1]	Y	Y	N	Y	M	N	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Macedonia	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Madagascar	Y	Y	N	Y	M	N	Y	N		N	Y	Y	Y	N	Y	Y
Malawi	N	N	Y	Y	P	N	N	N		N	N	N	N	N	Y	Y
Malaysia	Y	Y	N	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Maldives	Y	N	N	N	M	N	Y	N		N		Y	N	Y	Y	Y
Mali	Y	Y	N	Y	M	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Malta	Y	Y	N	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Marshall Islands	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y
Mauritania	Y	Y	Y	Y	P	N	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Mauritius	Y	Y	N	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Mexico	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Micronesia	Y	Y	N	Y	M	N	Y	N	Y	N	Y	N	Y	N	Y	Y
Moldova	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Monaco	Y	Y	N	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Mongolia	Y	N	N	Y	M	N	Y	N	N	N	N	Y	Y	Y	Y	Y
Montenegro	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Montserrat[2]	Y	Y	N	Y	M	N	Y	Y	Y	N	Y	Y	Y	Y	Y	N
Morocco	Y	Y	N	Y	M	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y
Mozambique	Y	Y	Y	Y	M	N	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
Namibia	Y	Y	Y	Y	M	N	Y	N	N	Y	Y	Y	Y	N	N	N
Nauru	Y	Y	N	Y	M	N	Y	Y	Y	N	Y	Y	Y	Y	N	Y

[1] The People's Republic of China extended the UN Financing of Terrorism Convention to the Special Administrative Regions of Hong Kong and Macau.

[2] The UK extended its application of the 1988 Convention and the UK Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Montserrat, the Turks and Caicos, Isle of Man, Bailiwick of Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions (NMP)	Egmont Financial Intelligence Units	System for Identifying/Forfeiting Assets	Arrangements for Asset Sharing	Cooperates w/International Law Enf.	International Transportation of Currency	Mutual Legal Assistance	Non-Bank Financial Institutions	Disclosure Protection "Safe Harbor"	Criminalized Financing of Terrorism	States Party to 1988 UN Convention	Intl. Terrorism Financing Convention
Nepal	Y	N	N	Y	M	N	N	N	Y	Y	Y	Y	N	Y	Y	N
Netherlands	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Netherlands Antilles	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
New Zealand	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Nicaragua	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	N	N	Y	Y	Y
Niger	Y	Y	N	Y	M	N	Y	N	Y	N	N	Y	N	N	Y	Y
Nigeria	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Niue	Y	Y	N	Y	M	Y	Y	N	Y	N	Y	Y	Y	N	NA	NA
Norway	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Oman	Y	Y	Y	Y	M	N	Y	N	Y	N	Y	Y	Y	Y	Y	N
Pakistan	Y	Y	Y	Y	M	N	Y	N	N	N	Y	Y	Y	Y	Y	N
Palau	Y	Y	Y	Y	M	N	Y	Y	Y	Y	Y	Y	Y	Y	N	Y
Panama	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Papua New Guinea	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y
Paraguay	Y	Y	Y	Y	M	Y	N	N	Y	Y	Y	Y	Y	N	Y	Y
Peru	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Philippines	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Poland	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y
Portugal	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Qatar	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Romania	Y	Y	Y	Y	M	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Russia	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Rwanda	N	N	N	N	P	N	N	N	Y	N	N	N	N	N	Y	Y
Samoa	Y	Y	Y	Y	M	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
San Marino	Y	Y	N	Y	M	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Sao Tome & Principe	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions (NMP)	Egmont Financial Intelligence Units	System for Identifying/Forfeiting Assets	Arrangements for Asset Sharing	Cooperates w/International Law Enf.	International Transportation of Currency	Mutual Legal Assistance	Non-Bank Financial Institutions	Disclosure Protection "Safe Harbor"	Criminalized Financing of Terrorism	States Party to 1988 UN Convention	Intl. Terrorism Financing Convention
Saudi Arabia	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Senegal	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	N	Y	Y
Serbia	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Seychelles	Y	Y	N	Y	M	N	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Sierra Leone	Y	Y	Y	Y	M	N	Y	N	N	Y	Y	Y	Y	Y	Y	Y
Singapore	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Slovakia	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Slovenia	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Solomon Islands	Y	Y	N	Y	N	N	N	N	N	N	N	N	N	N	N	N
South Africa	Y	Y	N	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Spain	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Sri Lanka	Y	N	N	Y	M	N	N	N	N	Y	Y	Y	Y	Y	Y	Y
St Kitts & Nevis	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
St. Lucia	Y	Y	N	Y	M	N	Y	N	Y	Y	Y	Y	Y	N	Y	N
St. Vincent/Grenadines	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Suriname	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	N	Y	N
Swaziland	Y	Y	Y	Y	M	N	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Sweden	Y	Y	Y	Y	M	Y	Y		Y	N	Y	Y	Y	Y	Y	Y
Switzerland	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Syria	Y	Y	Y	Y	M	Y	Y	N	N	N	Y	Y	N	N	Y	Y
Taiwan	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	N	NA	NA
Tajikistan	Y	Y	N	N	N	N	N	N	N	Y	Y	N	N	Y	Y	Y
Tanzania	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Thailand	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Togo	Y	N	Y	Y	N	N	Y	N	Y	N	Y	N	Y	Y	Y	Y

Actions by Governments	Criminalized Drug Money Laundering	Criminalized Beyond Drugs	Record Large Transactions	Maintain Records Over Time	Report Suspicious Transactions (NMP)	Egmont Financial Intelligence Units	System for Identifying/Forfeiting Assets	Arrangements for Asset Sharing	Cooperates w/International Law Enf.	International Transportation of Currency	Mutual Legal Assistance	Non-Bank Financial Institutions	Disclosure Protection "Safe Harbor"	Criminalized Financing of Terrorism	States Party to 1988 UN Convention	Intl. Terrorism Financing Convention
Tonga	Y	Y	Y	Y	M	N	Y	N	Y	Y	N	N	N	N	Y	Y
Trinidad & Tobago	Y	Y	Y	Y	M	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Tunisia	Y	Y	Y	Y	M	N	Y	N	Y	N	Y	Y	Y	Y	Y	Y
Turkey	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Turkmenistan	Y	Y	N	Y	M	N	Y	N	Y	Y	Y	N	N	Y	Y	Y
Turks & Caicos[1]	Y	Y	Y	Y	M	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N
Uganda	Y	N	N	N	M	N	N	N	Y	N	N	N	Y	Y	Y	Y
Ukraine	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
United Arab Emirates	Y	Y	Y	Y	M	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
United Kingdom	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
United States	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Uruguay	Y	Y	Y	Y	M	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Uzbekistan	Y	Y	N	Y	N	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y
Vanuatu	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Venezuela	Y	Y	Y	Y	M	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
Vietnam	Y	Y	Y	Y	M	N	Y	N	N	Y	Y	Y	N	N	Y	Y
Yemen	Y	Y	N	Y	M	N	N	N	Y	N	Y	Y	Y	N	Y	N
Zambia	Y	Y	N	Y	M	N	Y	N	Y	N	Y	N		N	Y	N
Zimbabwe	Y	Y	N	Y	M	N	Y	N	N	Y	N	N	N	Y	Y	N

[1] The UK extended its application of the 1988 Convention and the UK Terrorism Order 2001 to Anguilla, Bermuda, the British Virgin Islands, the Cayman Islands, Montserrat, the Turks and Caicos, Isle of Man, Bailiwick of Jersey, and Guernsey. The International Convention for the Suppression of the Financing of Terrorism has not yet been so extended.

Country Reports

Afghanistan

Afghanistan is not a regional financial or banking center, and is not considered an offshore financial center. However, its formal financial system is expanding rapidly while its traditional informal financial system remains significant in reach and scale. Afghanistan remains a major drug trafficking and drug producing country and the illicit narcotics trade is the primary source of laundered funds. Afghanistan enacted anti-money laundering and terrorist financing laws through presidential decree in October 2005. These laws are currently pending approval in parliament. While efforts continue to strengthen police and customs forces, there remain few resources, limited capacity, little expertise and insufficient political will to seriously combat financial crimes. The most fundamental obstacles continue to be legal, cultural and historical factors that conflict with more Western-style proposed reforms to the financial sector. Public corruption is also a significant problem. Afghanistan ranks 176 out of 180 countries in Transparency International's 2008 Corruption Perception Index.

According to United Nations Office of Drug Control (UNODC) statistics, opium poppy cultivation declined 19 percent in 2008. Poppy free provinces rose from 13 to 18. Despite these successes, Afghanistan still accounts for over 90 percent of the world's opium production. Opium gum is sometimes used as a currency—especially by rural farmers—and is used to store value in prime production areas. It is estimated that at least one third of Afghanistan's (licit plus illicit) gross domestic product (GDP) is derived directly from narcotics activities, and proceeds generated from the drug trade have reportedly fueled a growing real estate boom in Kabul, as well as a sharp increase in capital investment in rural poppy growing areas.

The majority of opium production comes from Taliban provincial strongholds in primarily the southern part of the country. The Taliban impose taxes on farmers and narcotics dealers, which undoubtedly helps finance their insurgency activities. Additional revenue streams for the Taliban and regional warlords come from "protecting" opium shipments, running heroin labs, and from "toll booths" established on transport and smuggling routes.

Afghan opium is refined into heroin by a growing number of production labs established within Afghanistan's borders. The heroin is then often broken into small shipments and smuggled across porous borders for resale abroad. Payment for the narcotics outside the country is facilitated through a variety of means, including through conventional trade and the traditional hawala system. In addition, the narcotics themselves are often used as tradable goods and as a means of exchange for automobiles, construction materials, foodstuffs, vegetable oils, electronics, and other goods between Afghanistan and neighboring Pakistan and Iran. Many of these goods are smuggled into Afghanistan from neighboring countries, particularly Iran and Pakistan, or enter via the Afghan Transit Trade Agreement (ATTA) without payment of customs duties or tariffs. Invoice fraud, corruption, indigenous smuggling networks, underground finance, and legitimate commerce are all intertwined.

Afghanistan is widely served by the hawala system, which provides a range of financial and nonfinancial business services in local, regional, and international markets. It is estimated that between 80 percent and 90 percent of all financial transfers in Afghanistan are made through hawala. Financial activities include foreign exchange transactions, funds transfers (particularly to and from neighboring countries with weak regulatory regimes for informal remittance systems), micro and trade finance, as well as some deposit-taking activities. Hawala is a traditional form of finance and is deeply entrenched and widely used throughout Afghanistan and the neighboring region. Although the hawala system and formal financial sector are distinct, the two systems have links. Hawala dealers often keep accounts at

banks and use wire-transfer services, while banks will occasionally use hawaladars to transmit funds to hard-to-reach areas within Afghanistan.

There are some 300 known hawala dealers in Kabul, with branches or additional dealers in each of the 34 provinces. There are approximately 1,500 dealers spread throughout Afghanistan that vary in size and reach. Primary hawala hubs include: Jalalabad, Kandahar, Herat, and Mazar-e-Sharif. These dealers are organized into informal provincial unions or guilds whose members maintain a number of agent-principal and partnership relationships with other dealers throughout the country and internationally. Their record keeping and accounting practices are robust and take note of currencies traded, international pricing, deposit balances, debits and credits with other dealers, lending, cash on hand, etc. Hawaladars are required to be licensed. To address this requirement, Da Afghanistan Bank (DAB) the Central Bank of Afghanistan, issued a new money service provider regulation in 2006 that streamlined the licensing process and substantially reduced the ongoing compliance burden for hawaladars. The focus of the regulation is largely on anti-money laundering and counterterrorist financing (AML/CTF). The regulation requires and provides standard mechanisms for record keeping and reporting of large transactions. The DAB is currently studying ways to improve the licensing process and streamline the reporting process, which is largely paper-based. In Kabul, 110 licenses have been issued under the regulation, which is the result of DAB outreach, law enforcement actions, and pressure from commercial banks where hawaladars hold accounts. However, DAB supervision beyond Kabul remains limited and presents an important regulatory challenge. In response, the DAB has begun outreach efforts to money service providers in other large cities, including Jalalabad, Mazar-e-Sharif and Herat, and hopes to expand the licensing to these cities in 2009. Given how widely used the hawala system is in Afghanistan, financial crimes undoubtedly occur through these entities.

The Anti-Money Laundering and Proceeds of Crime and Combating the Financing of Terrorism laws incorporate provisions that are designed to meet the recommendations of the Financial Action Task Force (FATF). These laws address the criminalization of money laundering and the financing of terrorism, customer due diligence, the establishment of a financial intelligence unit (FIU), international cooperation, extradition, and the freezing and confiscation of funds. Under the law, money laundering and terrorist financing are criminal offences. The AML law also includes provisions to address cross-border currency reporting, and establishes authorities to seize and confiscate monies found to be undeclared or falsely declared, or determined to be transferred for illicit purposes.

Under the AML, the Financial Transactions and Reports Analysis Center of Afghanistan (FinTRACA), Afghanistan's FIU, was established and functions as a semi-autonomous unit within the DAB. The FIU was opened in October 2005 with the assignment of a General Director, office space, and other basic resources. Since 2005, the FIU has expanded its operations into a new, secure building and added new analysts and law enforcement liaison officers.

Banks and other financial and nonfinancial institutions are required to report to the FIU all suspicious transactions (of any value) and large cash transactions above the equivalent of $10,000, as prescribed by the DAB. These financial institutions are also required to maintain their records for a minimum of 10 years. Approximately 22,000-25,000 large cash transaction reports are received from financial institutions and processed each month. This is a significant increase from last year and a clear indicator that financial flows through the formal financial system are gaining ground. The FIU currently has on record close to 500,000 large transaction reports. These reports are stored in a sophisticated and secure database that can be searched using a number of criteria. The FIU has the legal authority to freeze financial assets for up to seven days. FinTRACA also has access to records and databases of other government entities and the FIUs of other nations through information sharing agreements. Currently, FinTRACA has information sharing agreements with the following countries: Belarus, Kyrgyz Republic, Russia, Turkey, Sri Lanka, and the United Kingdom. FinTRACA is not yet a member of the Egmont Group.

The formal banking sector consists of fifteen licensed banks. AML examinations have been conducted for all these banks that have resulted in a growing awareness of AML requirements, deficiencies among the banks, and a need for building the AML capacity of the formal financial sector. Additionally, the Central Bank has worked with the banking community through the Afghan Bankers Association (ABA) to develop several ongoing topical working groups focused on AML issues. Recent ABA meetings have centered on the ensuring that banks submit suspicious transaction reports (STRs) in higher numbers and of better quality. Twenty-seven STRs were received in 2008, several of which were referred to law enforcement for investigation. By comparison, the FIU received seven STRs in 2007. Despite the increase in STR reporting, new workshops are planned to address this issue further in 2009.

The Afghanistan Central Bank has circulated a list of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list of designated individuals and entities to financial institutions. There is no information currently available regarding the results of these lists being circulated. Many banks also run their own compliance software to screen customers against UN and OFAC lists.

The Supervision Department within the DAB was formed at the end of 2003 and has been reorganized several times since then. The Supervision Department is currently divided into five divisions: Licensing, General Supervision (which includes on-site and off-site supervision), Special Supervision (which deals with special cases of problem banks), Regulation, and AML/CTF compliance. The AML/CTF compliance division is the newest addition. It is responsible for conducting examinations, overseeing money service providers, and conducting outreach to the commercial banking sector in the area of AML/CTF. Despite recent changes, the effectiveness of the Supervision Department in the AML area remains limited due to staffing, disjointed organization, and ongoing management issues. As a result, FinTRACA has taken on some supervisory responsibilities, yet resources at the FIU are limited for this task.

The Ministry of Interior (MOI) and the Attorney General's Office (AGO) are the primary financial enforcement and investigative authorities. They are responsible for tracing, seizing and freezing assets. While MOI generally has adequate police powers, it lacks specialized knowledge in financial crimes enforcement and the resources to trace, seize, and freeze assets. According to DAB, it is not aware of Afghanistan freezing, seizing, or forfeiting related assets in 2008. To address this area of concern, FinTRACA is building on an existing MOU with the MOI for cooperation and currently shares information with the Sensitive Investigations Unit (SIU), a law enforcement group within the MOI. Moreover, FinTRACA recently signed an MOU with the AGO and is awaiting finalization of another information sharing agreement with the National Directorate of Security (NDS).

Pursuant to the Central Bank law, a Financial Services Tribunal was established to review certain decisions and orders of the DAB. As part of its duties, the Tribunal reviews supervisory actions of the DAB, but does not prosecute cases of financial crime. At present, all financial crime cases are being forwarded to the Kabul Provincial Court where there has been limited activity in the past several years. The process to prosecute and adjudicate cases is long and cumbersome, significantly underdeveloped, and corruption often plays an important role across various levels. Afghanistan did not prosecute anyone for terrorist financing or money laundering in 2008.

Border security continues to be a major issue throughout Afghanistan. At present there are 14 official border crossings that have come under central government control, utilizing international donor assistance as well as local and international forces. However, many of the border areas are under policed or not policed at all. These areas are therefore susceptible to illicit cross-border trafficking, trade-based money laundering, and bulk cash smuggling. Furthermore, officials estimate that there are over 1,000 unofficial border crossings along Afghanistan's porous border. Customs authorities, with the help of outside assistance, have made important improvements, but much work remains to be done.

Customs collection and enforcement has improved in some areas and remained static in others, but smuggling and corruption continue to be major concerns, as well as trade fraud, which includes false and over-and under-invoicing. Thorough cargo inspections are not conducted at any official or unofficial border crossing. However, a new pilot program is underway at Islam Qalah (a key border crossing point between Iran and Afghanistan) to search suspected cargo. In addition, a pilot program is underway for declaring large, cross-border currency transactions at the Kabul International Airport (KIA). This prototype serves as the foundation for expansion to other land and air crossings. Currently, KIA requires incoming and outgoing passengers to fill out declarations forms for carrying cash in an amount of 1 million Afghanis (approximately $20,000) or its equivalent. There is no restriction on transporting any amount of declared currency. The DAB is working with Customs authorities to further improve enforcement of airport declarations at KIA and other international airports in country. Currently, cash smuggling reports from KIA are entered into the Customs database. This Customs data is shared with the FIU for analysis. To address cash smuggling at the border, the DAB sent delegations to key border crossings to assess capacity and describe the provisions of the law to the local authorities. Serious commitment is needed to adequately police the border to detect and intercept bulk cash smuggling.

Under the Law on Combating the Financing of Terrorism, any nonprofit organization that wishes to collect, receive, grant, or transfer funds and property must be entered in the registry with the Ministry of Auqaf (Islamic Affairs). All nonprofit organizations are subject to a due diligence process which includes an assessment of accounting, record keeping, and other activities. However, the capacity of the Ministry to conduct such examinations is extremely weak, and the reality is that any organization applying for a registration is granted one. Furthermore, because no adequate enforcement authority exists, many organizations operating under a nonprofit status in Afghanistan go completely unregistered, and illicit activities are suspected on the part of a number of organizations.

The Government of Afghanistan (GOA) is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Afghanistan has signed, but not yet ratified the UN Convention against Corruption (UNCAC). Ratification of UNCAC and amendment of domestic laws to conform to the UNCAC's obligations, among the benchmarks established under the London Compact, remain pending. In July 2006, Afghanistan became a member in the Asia Pacific Group, a FATF-Style Regional Body (FSRB), and has also obtained observer status in the Eurasian Group, another FSRB. No mutual evaluation has been conducted on the AML/CTF regime of Afghanistan to date; however, the APG is scheduled to assess the financial system in the third quarter of 2009.

The Government of Afghanistan has made progress over the past year in developing its overall AML/CTF regime. Recent improvement includes encouraging steps at the FIU, an increase in the reporting of large cash transactions, active participation in international AML bodies, continued work to improve AML compliance awareness among Afghan banks, and development and integration of information technology systems. However, Afghanistan must commit additional resources and find the political will to aggressively combat financial crimes, including corruption. Increasing the capacity of the DAB Supervision Department to conduct onsite AML/CTF supervision must be a priority. This should include both the formal and informal banking sectors. Specifically, the GOA must develop, staff, and fund a concerted effort to bring hawaladars into compliance in Kabul and major areas of commerce. As part of this effort, Afghanistan is developing secure, reliable, and capable relationships among departments and agencies involved in law enforcement. Afghanistan should also continue efforts to develop the investigative capabilities of law enforcement authorities in various areas of financial crimes, particularly money laundering and terrorist finance. Judicial authorities must also become proficient in understanding the various elements required for money laundering prosecutions. The FIU should become autonomous and increase its staff and resources. Afghan customs authorities should implement cross-border currency reporting and learn to recognize forms of trade-based money

laundering. Border enforcement should be a priority, both to enhance scarce revenue and to disrupt narcotics trafficking and illicit value transfer. Afghanistan should ratify the UN Convention against Corruption and make corresponding changes in its domestic laws.

Albania

Albania is not considered an important regional financial or offshore center. As a transit country for trafficking in narcotics, arms, contraband, and humans, Albania remains at significant risk for money laundering. The major sources of criminal proceeds in the country are trafficking offenses, official corruption, and fraud. Albania continues to be a source country for human trafficking. Corruption and organized crime are likely the most significant sources of money laundering, but the exact extent to which these various illegal activities contribute to overall crime proceeds and money laundering is unknown. The European Commission's (EC) November 2008 progress report on Albania identifies corruption, judicial deficiencies, politicization of the civil service, and organized crime as the biggest problems in Albania. The report also says money laundering, organized crime, and drug-trafficking are "serious concerns," stating that Albania has made "limited progress" in its fight against organized crime and money laundering.

Criminals frequently invest tainted money in real estate and business development projects. Because of its high level of consumer imports and weak customs controls, Albania has a significant black market for certain smuggled goods such as tobacco, jewelry, and mobile phones. Organized crime groups use Albania as a base of operations for conducting criminal activities in other countries and often return their illicit gains to Albania.

Because Albania's economy, particularly the private sector, remains largely cash-based, the proceeds from illicit activities are easily laundered in Albania. Albanian customs authorities report that organized criminal elements launder their illegal proceeds by smuggling bulk cash into and out of Albania by using international trade and fraudulent practices through import/export businesses. According to the Bank of Albania (the Central Bank), 23 percent of the money in circulation is outside of the banking system, compared to an average of ten percent in other Central and Eastern European transitioning economies. A significant portion of remittances enters the country through unofficial channels. It is estimated only half of total remittances enter Albania through banks or money transfer companies. The Central Bank estimates that in 2007, remittances comprised nearly 14 percent of Albania's annual gross domestic product (GDP). Black market exchange is still present in the country. However, it is declining steadily as a result of concerted efforts by the Government of Albania (GOA) to impede such exchanges. The Bankers Association estimates about half of all financial transactions take place through formal banking channels. Similarly, the GOA estimates proceeds from the informal sector account for approximately 30-60 percent of Albania's GDP. Although current law permits free trade zones, none are currently in operation.

The GOA is committed to fighting informality in the financial sector. There are 17 banks in Albania, and most of them have expanded both their national presence and the variety of services they offer. Electronic and automated teller machine (ATM) transactions are growing, especially in the urban areas, as more banks introduce this technology. ATM and debit and credit card usage expanded after the GOA decided to deliver public administration salaries through electronic transfers in 2005, and then compelled the private sector to follow suit in 2007. A May 2007 ruling also requires the private sector to channel at least 90 percent of its transactions through the banking sector. As of August 2008, 710,000 cards have been issued, almost entirely debit cards, but only a small number of people possess them and usage is primarily limited to a few large vendors.

Albania criminalizes money laundering through Article 287 of the Albanian Criminal Code of 1995, as amended. Albania's original money laundering law is "On the Prevention of Money Laundering," Law No. 8610 of May 17, 2000. In June 2003, Parliament approved Law No. 9084, which strengthens

Law No. 8610 and improves the Criminal Code and the Criminal Procedure Code. Law No. 9084 redefines the legal concept of money laundering, revises its definition to harmonize it with international standards, outlaws the establishment of anonymous accounts, and permits the confiscation of accounts. The law also mandates the identification of beneficial owners and places reporting requirements on both financial institutions and individuals. According to the law, obliged institutions are required to report to Albania's financial intelligence unit (FIU) all transactions exceeding $20,000 as well as those transactions that involve suspicious activity, regardless of amount. Currently, no law criminalizes negligence by financial institutions in money laundering cases.

In 2006, the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), a Financial Action Task Force (FATF)-style regional body, conducted a mutual evaluation of Albania's anti-money laundering/counterterrorist financing (AML/CTF) regime. In an attempt to address the many deficiencies identified by MONEYVAL, in May 2008, the Albanian Parliament passed Law No. 9917, "On Money Laundering and Terrorist Financing." The law entered into force in September 2008. The new anti-money laundering (AML) law lowers the reporting threshold for cash transactions from $20,000 to $15,000. Law No. 9917 strengthens customer due diligence (CDD) requirements by requiring the identification of all customers regardless of the size of their transactions, mandating that reporting subjects maintain on-going due diligence of clients according to the know-your-customer (KYC) concept, and establishing the requirement to perform enhanced due diligence on a risk sensitive basis. The law also includes a better definition of "client" to include any natural or legal person that is party to a business relationship, and mandates that CDD measures apply in transactions where terrorist financing is suspected. The law also increases the number of reporting entities, clarifies record keeping requirements, and better defines the responsibilities of the FIU.

Covered transactions must be reported within 72 hours of their occurrence. Individuals and entities reporting transactions are protected by law if they cooperate with and provide financial information to the FIU and law enforcement agencies. Reportedly, however, leaks of financial disclosure information from other agencies have compromised client confidentiality.

The Central Bank has established a task force to confirm banks' compliance with customer verification rules. It is the responsibility of the licensing authority to supervise intermediaries for compliance with AML regulations. For example, the Ministry of Justice is responsible for oversight of attorneys and notaries, and the Ministry of Finance (MOF) for accountants. Although regulations also cover nonbank financial institutions, enforcement remains poor in practice. There is an increasing number of suspicious transaction reports (STRs) coming from banks as that sector matures. A large number of STRs continue to come from tax and customs authorities and foreign counterparts.

Individuals must report to customs authorities all cross-border transactions that exceed approximately $10,000. Reportedly, Albania provides declaration forms at border crossing points but apparently only to those individuals who voluntarily make a declaration that would require completing the form. The law does not distinguish between an Albanian and a foreign visitor. However, customs controls on cross-border transactions lack effectiveness due to a lack of resources, poor training and, reportedly, corruption of customs officials.

Law No. 8610 establishes an administrative FIU, the General Directorate for the Prevention of Money Laundering (DPPPP), to coordinate the GOA's efforts to detect and prevent money laundering. Under Law No. 9084, the FIU became a quasi-independent agency within the Ministry of Finance. Albania is in the process of preparing a new administrative law on FIU operations. Referred to as the "draft law," it will clarify certain AML measures and elaborate on reporting requirements for obliged entities. As an administrative-type FIU, the DPPPP does not have law enforcement capabilities. The FIU receives reports from obligated entities, analyzes them, and then disseminates the results of its analysis to the Prosecutor's Office. Despite improvements of facilities and equipment, the Albanian FIU continues to

face many operational obstacles. The FIU's capacity remains limited as staff turnover is a persistent problem, and coordination and cooperation with the Prosecutor's Office remains problematic.

Since 2005, the FIU has referred to the Prosecutors Office 24 cases of both money laundering and terrorist financing, eight of which were reported during the first nine months of 2008. One case of money laundering has been prosecuted and currently there are two cases ready to be sent to the court. However, prosecution was declined for the rest. In January 2008, the first terrorist financing criminal case began in the First Instance Court for Serious Crimes. The case is against a Jordanian citizen accused of concealing funds allegedly intended to finance terrorism.

Albania's law sets forth an "all crimes" definition for the offense of money laundering, however, the Albanian court system applies a difficult burden of proof. Albanian courts require a conviction for the predicate offense before issuing an indictment for money laundering. In an effort to increase money laundering prosecutions, in May 2007, Albania established the Economic Crimes and Corruption Joint Investigative Unit (ECCJIU) within the Tirana District Prosecutors Office. This unit focuses efforts and builds expertise in the investigation and prosecution of financial crimes and corruption cases by bringing together members of the General Prosecutors Office, the Albanian State Police's Financial Crimes Sector, the MOF's Customs Service and Tax Police, and Albanian intelligence services. The ECCJIU also cooperates with the FIU and the National Intelligence Service. The ECCJIU has responsibility for the prosecution of money laundering cases within the District of Tirana.

Albania passed comprehensive legislation against organized crime in 2004. Law No. 9284, the "anti-mafia law," enables civil asset sequestration and confiscation provisions in cases involving organized crime and trafficking. The law applies to the assets of suspected persons, their families, and close associates. In cases where the value of the defendant's assets exceeds the income generated by known legal activity, the law places the burden on the defendant to prove a legitimate source of income to support the volume of assets. During the first half of 2008, the Serious Crimes Prosecution Office rendered eight sequestration and confiscation decisions pursuant to the anti-mafia law. The properties sequestered include one hotel and $7,000 in cash. The properties confiscated include $13,000 in cash and bank accounts, seven vehicles, and a coffee bar. The Agency for the Administration of the Sequestration and Confiscation of Assets (AASCA) was created in 2004, and is charged with the responsibility of administering confiscated assets. So far the agency has failed to function in a meaningful fashion. However, in response to pressure from U.S. government officials, the agency has started to perform better and has effectively taken control over several properties.

Article 230/a of the Penal Code criminalizes terrorist financing. The financing of terrorism, or its support of any kind, is punishable by a term of imprisonment of at least 15 years, and carries a fine of $50,000 to $100,000. The Penal Code also contains additional provisions dealing with terrorist financing, including sections dealing with disclosing information regarding an investigation or identification to identified persons and conducting financial transactions with identified persons. In an effort to make Albania's terrorist financing legislation comply more fully with international standards, the GOA, in 2007, amended its penal code to include a more specific definition for terrorist organizations. In addition, actions for terrorist purposes were identified and Albania's jurisdiction in terrorist financing cases was extended to include both resident and nonresident foreign citizens.

In 2004, Albania enacted Law No. 9258, "On Measures against Terrorist Financing." This law provides a mechanism for the sequestration and confiscation of assets belonging to terrorist financiers, particularly with regard to the United Nations (UN) updated lists of designees. While comprehensive, it lacks implementing regulations and thus is not fully in force. As of June 2008, the MOF claimed to maintain asset freezes against six individuals and 14 foundations and companies on the UN Security Council's 1267 Committee's consolidated lists of identified terrorist entities. In total, assets worth more than $10,000,000, belonging to six persons, five foundations and nine companies, remain sequestered, including 83 bank accounts containing more than $3,950,000; 18 apartments in an

expensive high rise apartment building in the center of Tirana; and several other properties throughout Albania. The full extent of sequestered assets is unknown.

The MOF is the main entity responsible for issuing freeze orders. After the MOF executes an order, the FIU circulates it to other government agencies, which then sequester any discovered assets belonging to the UNSCR 1267 named individual or entity. The sequestration orders remain in force as long as the subject's name remains on the list.

Albania is a party to the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the 1988 UN Drug Convention. Albania is a member of MONEYVAL, and the FIU is a member of the Egmont Group. The FIU has signed memoranda of understanding with 31 countries, Turkey being the most recent.

Although there are continuing initiatives to improve Albania's capacity to deal with financial crimes and money laundering, the lack of positive results and apparent inability to adequately address program deficiencies continue to hamper progress. In addition, although the new AML law was adopted in May 2008, it is difficult to evaluate the effectiveness of the new measures as implementing regulations have not yet been passed. The Government of Albania must provide the competent authorities adequate resources to administer and enforce the AML/CTF measures included in the May 2008 law. Albania also should incorporate into AML legislation specific provisions regarding negligent money laundering, corporate criminal liability, comprehensive customer identification procedures, and the adequate oversight of money remitters and charities. Albania should remove the requirement of a conviction for the predicate offense before a conviction for money laundering can be obtained. The FIU, prosecutors and the ECCJIU should enhance their effectiveness through improved cooperation with one another and outreach to other entities. The FIU should take steps to achieve effective analysis of the large volume of currency transaction reports and STRs received. The GOA should enact its draft law on FIU operations and promulgate implementing regulations for all applicable laws as soon as possible. The GOS should ensure that those charged with pursuing financial crime increase their technical knowledge to include modern financial investigation techniques. The GOA should provide its police force with the means to adequately maintain and retrieve its case files and records. The link between criminal intelligence and investigations remains weak as there is a lack of coordination between the prosecutors and the police. Investigators and prosecutors should implement case management techniques, and prosecutors and judges need to become more conversant with the nuances of money laundering. The GOA should devise implementing regulations for Law 9258 regarding sequestration and confiscation of assets linked to terrorist financing so that it can be fully effective. The GOA also should improve the enforcement and enlarge the scope of its asset seizure and forfeiture regime, including fully funding and supporting the AASCA.

Algeria

Algeria is not a regional or offshore financial center. The extent of money laundering through formal financial institutions is thought to be minimal due to stringent exchange control regulations and an antiquated banking sector. The partial convertibility of the Algerian dinar enables the Bank of Algeria (Algeria's central bank) to monitor all international financial operations carried out by public and private banking institutions.

The Algerian unemployment rate hovers unofficially above 25 percent, and mostly affects males under 30. This contributes to the crime rate, particularly kidnapping, theft, extortion, drug trafficking, and arms and cigarette smuggling. In addition to general criminal activity, terrorism has been on the rise. Al-Qaida in the Islamic Maghreb (AQIM) has committed a number of suicide attacks, kidnappings, roadside bombs, and assassinations throughout the country as well as in Algiers.

Algeria first criminalized terrorist financing through the adoption of Ordinance 95.11 on February 24, 1994, making the financing of terrorism punishable by five to ten years of imprisonment. On February 5, 2005, Algeria enacted public law 05.01, entitled "The Prevention and Fight against Money Laundering and Financing of Terrorism." The law aims to strengthen the powers of the Cellule du Traitement du Renseignement Financier (CTRF), an independent financial intelligence unit (FIU) within the Ministry of Finance (MOF) created in 2002. This law seeks to bring Algerian law into conformity with international standards and conventions. It offers guidance for the prevention and detection of money laundering and terrorist financing, institutional and judicial cooperation, and penal provisions. The CTRF's leadership is composed of officials from the Ministries of Finance, Justice, Customs, Interior and the Central Bank.

Algerian financial institutions, as well as Algerian customs and tax administration agents, are required to report any activities they suspect of being linked to criminal activity, money laundering, or terrorist financing to CTRF and comply with subsequent CTRF inquiries. They are obligated to verify the identity of their customers or their registered agents before opening an account; they must also record the origin and destination of funds they deem suspicious. In addition, these institutions must maintain confidential reports of suspicious transactions and customer records for at least five years after the date of the last transaction or the closing of an account. Since 2004, 204 suspicious transaction reports (STRs) have been received by the CTRF. Of that number, two have been referred for prosecution, with one referral resulting in a conviction.

The 2005 legislation extends money laundering controls to specific, nonbank financial professions such as lawyers, accountants, stockbrokers, insurance agents, pension managers, and dealers of precious metals and antiquities. Provided information is shared with CTRF in good faith, the law offers immunity from administrative or civil penalties for individuals who cooperate with money laundering and terrorist finance investigations. Under the law, assets may be frozen for up to 72 hours on the basis of suspicious activity; such freezes can only be extended with judicial authorization. Financial penalties for noncompliance range from 50,000 to 5 million Algerian dinars (approximately $700 to $70,000). In addition to its provisions pertaining to money laundered from illicit activities, the law allows the investigation of terrorist-associated funds derived from "clean" sources.

The law provides significant authority to the Algerian Banking Commission, the independent body established under authority of the Bank of Algeria to supervise banks and financial institutions, to inform CTRF of suspicious or complex transactions. The law also gives the Algerian Banking Commission, CTRF, and the Algerian judiciary wide latitude to exchange information with their foreign government counterparts in the course of money laundering and terrorist finance investigations, provided confidentiality for suspected entities is insured. A clause excludes the sharing of information with foreign governments in the event legal proceedings are already underway in Algeria against the suspected entity, or if the information is deemed too sensitive for national security reasons.

In 2006, the Government of Algeria (GOA) decreed that payments exceeding a certain value must be made by check, wire transfer or other specified methods that are traceable, rather than in cash. However, a nation-wide electronic check-clearing system has been slow to develop, and actors in the government, banking system and business community have been split as to what the cash payment limit should be, and if exceptions should be made for certain vendors such as traders of vegetables and fish. While nonresidents would be exempt from the requirements, they would still be obliged (like all travelers to and from the country) to report foreign currency in their possession to the Algerian Customs Authority.

The Ministry of Interior is charged with registering foreign and domestic nongovernmental organizations in Algeria. While the Ministry of Religious Affairs legally controls the collection of

funds at mosques for charitable purposes, some of these funds undoubtedly escape the notice of government monitoring efforts.

There are reports that Algerian customs and law enforcement authorities are increasingly concerned with cases of customs fraud and trade-based money laundering. Other risk areas for financial crimes include unregulated alternative remittance and currency exchange systems; tax evasion; misuse of real estate transactions as a means of money laundering; commercial invoice fraud, and a cash-based economy. Most money laundering is believed to occur primarily outside the formal financial system, given the large percentage of financial transactions occurring in the informal gray and black economies.

Algerian authorities are taking steps to coordinate information sharing between concerned agencies. In 2008, the Ministry of Justice established a specialized cadre of investigators, prosecutors and judges who are being trained in the investigation and prosecution of financial crimes.

In November 2004, Algeria became a member of the Middle East and North Africa Financial Action Task Force (MENA FATF). Algeria is a party to the UN Convention against Transnational Organized Crime, the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Corruption, and the 1988 UN Drug Convention. In addition, Algeria is a signatory to various UN, Arab, and African conventions against terrorism, trafficking in persons, and organized crime.

The Government of Algeria has taken significant steps to enhance its statutory regime against anti-money laundering and terrorist financing. It needs to move forward now to implement those laws and eliminate bureaucratic barriers among various government agencies. The CTRF should be the focal point for anti-money laundering/counterterrorist finance (AML/CTF) suspicious transaction report analysis, which would require the CTRF to develop an in-house analytical capability. The CTRF should conduct outreach to the formal and informal financial sectors, adhere to international standards, and take steps to prepare for membership in the Egmont Group. In addition, given the scope of Algeria's informal economy, new emphasis should be made to identify value transfer mechanisms not covered in Algeria's AML/CTF legal and regulatory framework, and to limit the frequency and the size of cash transactions. Algerian law enforcement and customs authorities should enhance their ability to investigate trade-based money laundering, value transfer, and bulk cash smuggling used for financing terrorism and other illicit financial activities.

Angola

No new information was received for 2008. The following is a reprint of last year's report:

Angola is neither a regional nor an offshore financial center and has not prosecuted any known cases of money laundering. Angola does not produce significant quantities of drugs, although it continues to be a transit point for drug trafficking, particularly cocaine brought in from Brazil or South Africa destined for Europe. The laundering of funds derived from continuous and widespread high-level corruption is a concern, as is the use of diamonds as a vehicle for money laundering. The Government of the Republic of Angola (GRA) has implemented a diamond control system in accordance with the Kimberley Process. However, corruption and Angola's long and porous borders further facilitate smuggling and the laundering of diamonds.

Angola currently has no comprehensive laws, regulations, or other procedures to detect money laundering and financial crimes. Other provisions of the criminal code do address some related crimes. The various ministries with responsibility for detection and enforcement are revising a draft anti-money laundering law drawn up with help from the World Bank. The Central Bank's Supervision Division, which has responsibility for money laundering issues, exercises some authority to detect and suppress illicit banking activities under legislation governing foreign exchange controls. The Central Bank has the authority to freeze assets, but Angola does not presently have an effective system for

identifying, tracing, or seizing assets. Instead, such crimes are addressed through other provisions of the criminal code. For example, Angola's counternarcotics laws criminalize money laundering related to narcotics trafficking.

Angola's high rate of cash flow makes its financial system an attractive site for money laundering. With no domestic interbank dollar clearing system, even dollar transfers between domestic Angolan banks are logged as "international" transfers, thus creating an incentive to settle transfers in cash. The local banking system imports approximately U.S. $200-300 million in currency per month, largely in dollars, without a corresponding cash outflow. Local bank representatives have reported that clients have walked into banks with up to U.S. $2 million in a briefcase to make a deposit. No currency transaction reports cover such large cash transactions. These massive cash flows occur in a banking system ill-equipped to detect and report suspicious activity. The Central Bank has no workable data management system and only rudimentary analytic capability. Corruption pervades Angolan society and commerce and extends across all levels of government. Angola is rated 147 out of 180 countries in Transparency International's 2007 International Corruption Perception Index.

Angola is party to the 1988 UN Drug Convention and the UN Convention against Corruption. Angola has signed but has not yet ratified the UN Convention against Transnational Organized Crime. Angola has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Angola should pass its pending legislation to criminalize money laundering beyond drug offenses and terrorist financing. The GRA should establish a system of financial transparency reporting requirements and a corresponding Financial Intelligence Unit through legislation that adheres to world standards. The GRA should then move quickly to implement this legislation and bolster the capacity of law enforcement to investigate financial crimes. Angola's judiciary, including its Audit Court (Tribunal de Contas) should give priority to prosecuting financial crimes, including corruption. The GRA should become a party to both the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of the Financing of Terrorism. The GRA should increase efforts to combat official corruption, by establishing an effective system to identify, trace, seize, and forfeit assets and by empowering investigative magistrates to actively seek out and prosecute high profile cases of corruption.

Antigua and Barbuda

Antigua and Barbuda has comprehensive legislation in place to regulate its financial sector, but remains susceptible to money laundering due to its offshore financial sector and Internet gaming industry. Illicit proceeds from the transshipment of narcotics and from financial crimes occurring in the U.S. also are laundered in Antigua and Barbuda.

As of 2008, Antigua and Barbuda has eight domestic banks, seven credit unions, seven money transmitters, 18 offshore banks, two trusts, three offshore insurance companies, 2,967 international business corporations (IBCs), and 20 licensed Internet gaming companies. In addition, there are approximately 33 real estate agents, five casinos, and 14 dealers of precious metals and stones. The International Business Corporations Act of 1982 (IBCA), as amended, is the governing legal framework for offshore businesses in Antigua and Barbuda. Bearer shares are permitted for international companies. However, the license application requires disclosure of the names and addresses of directors (who must be naturalized persons), the activities the corporation intends to conduct, the names of shareholders, and number of shares they will hold. Registered agents or service providers are required by law to know the names of beneficial owners. Failure to provide information or giving false information is punishable by a fine of $50,000. Offshore financial institutions are exempt from corporate income tax. All licensed institutions are required to have a physical presence, which means presence of at least a full-time senior officer and availability of all files and records. Shell companies are not permitted.

The Money Laundering Prevention Act of 1996 (MLPA), as amended, is the cornerstone of Antigua and Barbuda's anti-money laundering legislation. The MLPA makes it an offense for any person to obtain, conceal, retain, manage, or invest illicit proceeds or bring such proceeds into Antigua and Barbuda if that person knows or has reason to suspect that they are derived directly or indirectly from any unlawful activity. The MLPA creates a Supervisory Authority. In 2003, the director of the Office of National Drug Control and Money Laundering Policy (ONDCP) was designated to act in this capacity. The MLPA covers institutions defined under the Banking Act, IBCA, and the Financial Institutions (Non-Banking) Act, which include offshore banks, IBCs, money transmitters, credit unions, building societies, trust businesses, casinos, Internet gaming companies, and sports betting companies. Intermediaries such as lawyers and accountants are not included in the MLPA. The MLPA requires reporting entities to report suspicious activity suspected to be related to money laundering, whether a transaction was completed or not. There is no reporting threshold imposed on banks and financial institutions. Internet gaming companies, however, are required by the Interactive Gaming and Interactive Wagering Regulations to report to the ONDCP all payouts over $25,000. The GOAB amended the MLPA in 2008 to provide for the licensing and regulation of money transmitters; enhance tipping off and record retention provisions; require financial institutions to review complex or unusual transactions whether the transaction was completed or not; and to extend power to seize and detain suspected currency to ONDCP officers.

Domestic casinos are required to incorporate as domestic corporations. Internet gaming companies are required to incorporate as IBCs, and as such are required to have a physical presence. Internet gaming sites are considered to have a physical presence when the primary servers and the key person are resident in Antigua and Barbuda. The Government of Antigua and Barbuda (GOAB) receives approximately $2,800,000 per year from license fees and other charges related to the Internet gaming industry. A nominal free trade zone in the country seeks to attract investment in areas deemed as priority by the government. Casinos and sports book-wagering operations in Antigua and Barbuda's free trade zone are supervised by the ONDCP, and the Directorate of Offshore Gaming (DOG), housed in the Financial Services Regulatory Commission (FSRC). The GOAB has adopted regulations for the licensing of interactive gaming and wagering, to address possible money laundering through client accounts of Internet gaming operations. The FSRC and DOG have also issued Internet gaming technical standards and guidelines. Internet gaming companies are required to submit quarterly and annual audited financial statements, enforce know-your-customer verification procedures, and maintain records relating to all gaming and financial transactions of each customer for six years. The GOAB does not have a unified regulatory structure or uniform supervisory practices for its domestic and offshore banking sectors. Currently, the Eastern Caribbean Central Bank (ECCB) supervises Antigua and Barbuda's domestic banking sector. The Registrar of Insurance supervises and examines domestic insurance agencies. The director of the ONDCP supervises all financial institutions for compliance with suspicious transaction reporting requirements. The FSRC is responsible for the regulation and supervision of all institutions licensed under the IBCA, including offshore banking and all aspects of offshore gaming. This includes issuing licenses for IBCs, maintaining the register of all corporations, and conducting examinations and reviews of offshore financial institutions as well as some domestic financial entities, such as insurance companies and trusts.

In the offshore sector, the IBCA requires that a corporate entity submit all books, minutes, cash, securities, vouchers, customer identification, and customer account records. Financial institutions are required to maintain records for six years after an account is closed. The IBCA provides for disclosure of confidential information pursuant to a request by the director of the ONDCP, and pursuant to an order of a court of competent jurisdiction in Antigua and Barbuda. In addition, the MLPA contains provisions for obtaining client and ownership information. Section 25 of the MLPA states the provisions of the Act shall have effect notwithstanding any obligation as to secrecy or other restriction upon the disclosure of information imposed by any law or otherwise.

The Office of National Drug Control and Money Laundering Policy Act, 2003 (ONDCP Act) establishes the ONDCP as the FIU. The ONDCP is an independent organization under the Ministry of National Security and is primarily responsible for the enforcement of the MLPA and for directing the GOAB's anti-money laundering efforts in coordination with the FSRC. In its role as the Supervisory Authority, the ONDCP fulfills the responsibilities described in the MLPA, which includes the supervision of all financial institutions with respect to filing suspicious transaction reports (STRs). STRs from domestic and offshore gaming entities are sent to the ONDCP and FSRC. As of December 2008, the ONDCP had received 73 STRs (increased from 43 in 2007), 14 of which were investigated. Additionally, the ONDCP Act authorizes the director to appoint officers to investigate narcotics-trafficking, fraud, money laundering, and terrorist financing offenses. Auditors of financial institutions review their compliance programs and submit reports to the ONDCP for analysis and recommendations. The ONDCP has no direct access to databases of financial institutions. Domestically, the ONDCP has a memorandum of understanding (MOU) with the FSRC and is expected to sign another with the ECCB. Other MOUs have been drafted to cover all aspects of the ONDCP's relationship with the Royal Antigua and Barbuda Police Force, Customs, Immigration, and the Antigua and Barbuda Defense Force. No arrests, prosecutions or convictions were reported by the GOAB in 2006 or 2007.

Under the MLPA, a person entering or leaving the country is required to report to the ONDCP whether he or she is carrying $10,000 or more in cash or currency. In addition, all travelers are required to fill out a customs declaration form indicating if they are carrying in excess of $10,000 in cash or currency. If so, they may be subject to further questioning and possible search of their belongings by Customs officers. The GOAB Customs Department maintains statistics on cross-border cash reports and seizures for failure to report. This information is shared with the ONDCP and the police. One arrest was made in January 2008, involving the undeclared importation of approximately $80,000 by a passenger at the airport who carried part of it in his hand luggage and the rest strapped around his waist.

The Misuse of Drugs Act empowers the court to forfeit assets related to drug offenses. The ONDCP is responsible for tracing, seizing and freezing assets related to money laundering. The ONDCP has the ability to direct a financial institution to freeze property for up to seven days, while it makes an application for a freeze order. If a charge is not filed or an application for civil forfeiture is not made within 30 days, the freeze order lapses. Convictions for a money laundering offense make it likely that an application for forfeiture will succeed unless the defendant can show the property was acquired by legal means or the defendant's business was legitimate. Forfeited assets are placed into the Forfeiture Fund and can be used by the ONDCP for any other purpose. Approximately 20 percent of forfeited assets go to the Consolidated Fund at the Treasury.

The GOAB has entered into an asset sharing agreement with Canada, and is currently working on asset sharing agreements with other jurisdictions, including the U.S. The director of ONDCP, with Cabinet approval, may enter into agreements and arrangements that cover matters relating to asset sharing with authorities of a foreign State. There are asset sharing agreements with some countries, while others are negotiated on an ad hoc basis. Regardless of its own civil forfeiture laws, currently the GOAB can only provide forfeiture assistance in criminal forfeiture cases, an anomaly which should be remedied.

In recent years, the GOAB has frozen approximately $6,000,000 in Antigua and Barbuda financial institutions as a result of U.S. requests and has repatriated approximately $4,000,000. The GOAB has frozen, on its own initiative, over $90,000,000 believed to be connected to money laundering cases still pending in the United States and other countries. The GOAB reported seizing $420,236 in 2006, $14,753 in 2007, and $81,601 in 2008.

The GOAB enacted the Prevention of Terrorism Act 2001(PTA), amended in 2005, to implement the UN conventions on terrorism. The PTA empowers the ONDCP to nominate any entity as a "terrorist entity" and to seize and forfeit terrorist funds. The law covers any finances in any way related to terrorism. The PTA also provides the authority for the seizure of property used in the commission of a terrorist act; seizure and restraint of property that has been, is being or may be used to commit a terrorism offence; forfeiture of property on conviction of a terrorism offence; and forfeiture of property owned or controlled by terrorists. The PTA requires financial institutions to report every three months on whether they are in possession of any property owned or controlled by or on behalf of a terrorist group. In addition, financial institutions must report every transaction suspected to be related to the financing of terrorism to the ONDCP. The GOAB amended the PTA in 2008 to provide the Supervisory Authority and the ONDCP the power to direct a financial institution to freeze property for up to seven days while the authority seeks a freeze order from the court. The amendment also includes provisions making it an offense for individuals to know and/or fail to disclose information leading to prevention of an attempt to commit a terrorist act. Those who conceal wrongdoings will be ordered to pay a penalty of $500,000.

The Attorney General may revoke or deny the registration of a charity or nonprofit organization if it is believed funds from the organization are being used for financing terrorism. The GOAB circulates lists of terrorists and terrorist entities to all financial institutions in Antigua and Barbuda. No known evidence of terrorist financing has been discovered in Antigua and Barbuda to date. The GOAB does not believe indigenous alternative remittance systems exist in the country, and has not undertaken any specific initiatives focused on the misuse of charities and nonprofit entities.

The GOAB continues its bilateral and multilateral cooperation in various criminal and civil investigations and prosecutions. As a result of such cooperation, both the United States and Canada have shared forfeited assets with the GOAB on several occasions. The amended Banking Act 2004 enables the ECCB to share information directly with foreign regulators if a MOU is established. In 1999, a Mutual Legal Assistance Treaty and an extradition treaty with the United States entered into force. An extradition request related to a fraud and money laundering investigation remains pending under the treaty. The GOAB signed a Tax Information Exchange Agreement with the United States in December 2001 that allows the exchange of tax information between the two nations.

Antigua and Barbuda is a member of the Caribbean Financial Action Task Force (CFATF), a Financial Action Task Force-style regional body, and underwent a mutual evaluation in June 2008. The evaluation notes several deficiencies in the GOAB's anti-money laundering/counterterrorist financing (AML/CTF) regime including: weak requirements for enhanced customer due diligence for high risk customers such as politically exposed persons; non-enforceable requirements for financial institutions to have policies and procedures in place to address specific risks associated with non-face-to-face customers; non-enforceable requirements prohibiting domestic and offshore banks from having correspondent banking relationships with shell banks; and wire transfer requirements not enforceable in accordance with the FATF Recommendations. Furthermore, the evaluation notes the GOAB needs to enact provisions to require financial institutions to develop internal controls and procedures to include terrorist financing; the supervisory authorities have not been given the responsibility for ensuring financial institutions adequately comply with AML/CTF requirements; and there are no measures in place to ensure that bearer shares under the IBCA are not misused for money laundering.

Antigua and Barbuda is also a member of the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD). The GOAB is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the UN Convention for the Suppression of the Financing of Terrorism. The ONDCP is a member of the Egmont Group.

The Government of Antigua and Barbuda has taken steps to combat money laundering and terrorist financing by passing relevant legislation that applies to both domestic and offshore financial institutions, and establishing a thorough regulatory regime. However, the GOAB should take steps to amend its legislation of cover intermediaries, enhanced due diligence for PEPs and other high-risk customers, and to provide for enforceable provisions on the prohibition of correspondent accounts for or with shell banks. The GOAB also should implement and enforce all provisions of its AML/CTF legislation, including the comprehensive supervision of its offshore sector and gaming industry. The ONDCP should be given direct access to financial institution records in order to effectively assess their AML/CTF compliance. Despite the comprehensive nature of the law, Antigua and Barbuda has yet to prosecute a money laundering case and there are few arrests or prosecutions. More comprehensive investigations could lead to higher numbers of arrests, prosecutions, and convictions. Continued efforts should be made to enhance the capacity of law enforcement and customs authorities to recognize money laundering typologies that fall outside the formal financial sector. Continued international cooperation, particularly with regard to the timely sharing of statistics and information related to offshore institutions, and enforcement of foreign civil asset forfeiture orders will likewise enhance Antigua and Barbuda's ability to combat money laundering.

Argentina

Argentina is neither an important regional financial center nor an offshore financial center. Money laundering related to narcotics trafficking, corruption, contraband, and tax evasion is believed to occur throughout the financial system, in spite of the efforts of the Government of Argentina (GOA) to stop it. Transactions conducted through nonbank sectors and professions, such as the insurance industry, financial advisors, accountants, notaries, trusts, and companies, real or shell, remain viable mechanisms to launder illicit funds. Tax evasion is the predicate crime in the majority of Argentine money laundering investigations.

Argentina has a long history of capital flight and tax evasion, and Argentines hold billions of dollars outside the formal financial system (both offshore and in-country), much of it legitimately earned money that was not taxed. To combat capital flight and to encourage the return of these undeclared billions, on December 18, 2008, Argentina's legislature approved a tax moratorium and capital repatriation law that would provide a tax amnesty for persons who repatriate undeclared offshore assets during a six-month window. The law entered into force December 24. Under the law, government tax authorities are prohibited from inquiring into the provenance of declared funds; and some critics have raised concerns that this could facilitate money laundering. Implementing regulations are to be promulgated in February 2009, which will clarify that transactions under this law will be subject to existing laws, rules, and regulations related to the prevention of financial crimes and will also reportedly include a requirement that transfers from abroad originate in countries that comply with international money laundering and terrorism financing standards. Top-level GOA officials have indicated that they will ensure all Argentine legislation, including this law, abides by Argentina's obligations as a member of the Financial Action Task Force (FATF) and the Financial Action Task Force for South America (GAFISUD). In January, the GOA takes over the Presidency of GAFISUD for 2009.

In 2007, the Argentine Congress passed legislation criminalizing terrorism and terrorist financing. Law 26.268, "Illegal Terrorist Associations and Terrorism Financing," amends the Penal Code and Argentina's anti-money laundering law, Law No. 25.246, to criminalize acts of terrorism and terrorist financing, and establish terrorist financing as a predicate offense for money laundering. Persons convicted of terrorism are subject to a prison sentence of five to 20 years, and those convicted of financing terrorism are subject to a five to 15 year sentence. The new law provides the legal foundation for Argentina's financial intelligence unit (the Unidad de Información Financiera, or UIF), Central Bank, and other regulatory and law enforcement bodies to investigate and prosecute such

crimes. With the passage of Law 26.268, Argentina joins Chile, Colombia, and Uruguay as the only countries in South America to have criminalized terrorist financing.

On September 11, 2007, former President Nestor Kirchner signed into force the National Anti-Money Laundering and Counter-Terrorism Finance Agenda. The overall goal of the National Agenda is to serve as a roadmap for fine-tuning and implementing existing money laundering and terrorist financing laws and regulations. The Agenda's 20 individual objectives focus on closing legal and regulatory loopholes and improving interagency cooperation. The ongoing challenge is for Argentine law enforcement and regulatory institutions to continue to implement the National Agenda and aggressively enforce the strengthened and expanded legal, regulatory, and administrative measures available to them to combat financial crimes.

Argentina's primary anti-money laundering legislation is Law 25.246 of May 2000 (although money laundering was first criminalized under Section 25 of Law 23.737, which amended Argentina's Penal Code in October 1989). Law 25.246 expanded the predicate offenses for money laundering to include all crimes listed in the Penal Code, set a stricter regulatory framework for the financial sectors, and created the UIF under the Ministry of Justice and Human Rights. The law requires customer identification, record-keeping, and reporting of suspicious transactions by all financial entities and businesses supervised by the Central Bank, the Securities Exchange Commission (Comisión Nacional de Valores, or CNV), and the National Insurance Superintendence (Superintendencia de Seguros de la Nación, or SSN). The law requires similar reporting by designated self-regulated nonfinancial entities that report to the UIF. Further, the law forbids institutions to notify their clients when filing suspicious transaction reports (STRs), and provides a safe harbor from liability for reporting such transactions. Reports that are deemed by the UIF to warrant further investigation are forwarded to the special anti-money laundering and counterterrorism finance prosecution unit of the Attorney General's Office.

Law 26.087 of March 2006 amends and modifies Law 25.246 to address many previous deficiencies in Argentina's anti-money laundering regime. It makes substantive improvements to existing law, including lifting bank, stock exchange, and professional secrecy restrictions on filing suspicious activity reports; partially lifting tax secrecy provisions; clarifying which courts can hear requests to lift tax secrecy requests; and requiring court decisions within 30 days. Law 26.087 also lowers the standard of proof required before the UIF can pass cases to prosecutors, and eliminates the so-called "friends and family" exemption contained in Article 277 of the Argentine Criminal Code for cases of money laundering, while narrowing the exemption in cases of concealment. Overall, the law clarifies the relationship, jurisdiction, and responsibilities of the UIF and the Attorney General's Office, and improves information sharing and coordination. The law also reduces restrictions that have prevented the UIF from obtaining information needed for money laundering investigations by granting greater access to STRs filed by banks. However, the law does not lift financial secrecy provisions on records of large cash transactions, which are maintained by banks when customers conduct a cash transaction exceeding 30,000 pesos (approximately $9,000).

In September 2006, Congress passed Law 26.119, which amends Law 25.246 to modify the composition of the UIF. The law reorganized the UIF's executive structure, changing it from a five-member directorship with rotating presidency to a structure that has a permanent, politically-appointed president and vice-president. Law 26.119 also established a UIF Board of Advisors, comprised of representatives of key government entities, including the Central Bank, AFIP, the Securities Exchange Commission, the National Counter-narcotics Secretariat (SEDRONAR), and the Justice, Economy, and Interior Ministries. The UIF legally must consult the Board of Advisors, although its opinions on UIF decisions and actions are nonbinding.

The UIF has issued resolutions widening the range of institutions and businesses required to report suspicious or unusual transactions beyond those identified in Law 25.246. Obligated entities include the tax authority (Administración Federal de Ingresos Publicos, or AFIP), Customs, banks, currency

exchange houses, casinos, securities dealers, insurance companies, postal money transmitters, accountants, notaries public, and dealers in art, antiques and precious metals. The resolutions issued by the UIF also provide guidelines for identifying suspicious or unusual transactions. All suspicious or unusual transactions, regardless of the amount, must be reported directly to the UIF. Obligated entities are required to maintain a database of information related to client transactions, including suspicious or unusual transaction reports, for at least five years and must respond to requests from the UIF for further information within a designated period. As of September 2008 the UIF had received 4,032 reports of suspicious or unusual activities since its inception in November 2002, forwarded 491 suspected cases of money laundering to prosecutors for review, and collaborated with judicial system investigations of 155 cases of suspected money laundering. There have been only two convictions for money laundering since it was first criminalized in 1989 under Article 25 of Narcotics Law 23.737 and none since the passage of Law 25.246 in 2000. A third money laundering case brought under Law 23.737 is pending before Argentina's Supreme Court.

The Central Bank requires by resolution that all banks maintain a database of all transactions exceeding 30,000 pesos, and submit the data to the Central Bank upon request. Law 25.246 requires banks to make available to the UIF upon request records of transactions involving the transfer of funds (outgoing or incoming), cash deposits, or currency exchanges that are equal to or greater than 10,000 pesos (approximately $3,200). The UIF further receives copies of the declarations to be made by all individuals (foreigners or Argentine citizens) entering or departing Argentina with over $10,000 in currency or monetary instruments. These declarations are required by Resolutions 1172/2001 and 1176/2001, which were issued by the Argentine Customs Service in December 2001. In 2003, the Argentine Congress passed a law that would have provided for the immediate fine of 25 percent of the undeclared amount, and for the seizure and forfeiture of the remaining undeclared currency and/or monetary instruments. However, the President vetoed the law because it allegedly conflicted with Argentina's commitments to MERCOSUR (Common Market of the Southern Cone).

Although the GOA has passed a number of new laws in recent years to improve its anti-money laundering and counterfinancing of terrorism (AML/CTF) regime, Law 25.246 still limits the UIF's role to investigating only money laundering arising from seven specific or "predicate" crimes. Also, the law does not criminalize money laundering as an offense independent of the underlying crime. A person who commits a crime cannot be independently prosecuted for laundering money obtained from the crime; only someone who aids the criminal after the fact in hiding the origins of the money can be guilty of money laundering. Another impediment to Argentina's anti-money laundering regime is that only transactions (or a series of related transactions) exceeding 50,000 pesos (approximately $16,000) can constitute money laundering. Transactions below 50,000 pesos can constitute only concealment, a lesser offense.

In 2006 and 2007, the National Coordination Unit in the Ministry of Justice, Security, and Human Rights became fully functional, managing the government's AML/CTF efforts and representing Argentina at the Financial Action Task Force (FATF), the Financial Action Task Force for South America (GAFISUD), and the Organization of American States Inter-American Control Commission (OAS/CICAD) Group of Experts. The Attorney General's special prosecution unit set up to handle money laundering and terrorism finance cases began operations in 2007. Although the Argentine Central Bank's Superintendent of Banks has not created a specialized anti-money laundering and counterterrorism finance examination program as previously considered, it began in 2008 specific anti-money laundering and counterterrorism finance inspections of financial entities and exchange houses.

Argentina's Narcotics Law of 1989 authorizes the seizure of assets and profits, and provides that these or the proceeds of sales will be used in the fight against illegal narcotics trafficking. Law 25.246 provides that proceeds of assets forfeited under this law can primarily be used to fund the UIF. Argentine courts and law enforcement agencies have used the authority to seize and utilize assets on a

selective and limited basis, although complex procedural requirements complicate authorities' ability to take full advantage of the asset seizure provisions offered under these laws.

Prior to the passage of terrorist financing legislation in June 2007, the Central Bank was the lead Argentine entity responsible for issuing regulations on combating the financing of terrorism. The Central Bank issued Circular A-4273 in 2005 (titled "Norms on 'Prevention of Terrorist Financing'"), requiring banks to report any detected instances of the financing of terrorism. The Central Bank regularly updates and modifies the original circular. The Central Bank of Argentina also issued Circular B-6986 in 2004, instructing financial institutions to identify and freeze the funds and financial assets of the individuals and entities listed on the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. It modified this circular with Resolution 319 in October 2005, which expands Circular B-6986 to require financial institutions to check transactions against the terrorist lists of the United Nations, United States, European Union, Great Britain, and Canada. No assets have been identified or frozen to date. The GOA and Central Bank assert that they remain committed to freezing assets of terrorist groups identified by the United Nations if detected in Argentine financial institutions.

In December 2006, the U.S. Department of Treasury designated nine individuals and two entities that provided financial or logistical support to Hizballah and operated in the territory of neighboring countries that border Argentina. This region is commonly referred to as the Tri-Border Area, located between Argentina, Brazil, and Paraguay. The GOA joined the Brazilian and Paraguayan governments in publicly disagreeing with the designations, stating that the United States had not provided new information proving terrorist financing activity is occurring in the Tri-Border Area.

Working with the U.S. Department of Homeland Security's Office of Immigration and Customs Enforcement (ICE), Argentina has established a Trade Transparency Unit (TTU). The TTU examines anomalies in trade data that could be indicative of customs fraud and international trade-based money laundering. One key focus of the TTU, as well as of other TTUs in the region, is financial crime occurring in the Tri-Border Area. The creation of the TTU was also a positive step toward complying with FATF Special Recommendation VI on terrorist financing via alternative remittance systems. Trade-based systems often use fraudulent trade documents and over and under invoicing schemes to provide counter valuation in value transfer and settling accounts.

The GOA remains active in multilateral counternarcotics and international AML/CTF organizations. It is a member of the OAS/CICAD Experts Group to Control Money Laundering, the FATF and GAFISUD. The GOA is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. Argentina participates in the "3 Plus 1" Security Group (formerly the Counter-Terrorism Dialogue) between the United States and the Tri-Border Area countries. The UIF has been a member of the Egmont Group since July 2003, and has signed memoranda of understanding regarding the exchange of information with a number of other financial intelligence units. The GOA and the U.S. government have a Mutual Legal Assistance Treaty that entered into force in 1993, and an extradition treaty that entered into force in 2000.

With passage of counterterrorist financing legislation and strengthened mechanisms available under Laws 26.119, 26.087, 25.246, and 26.268 Argentina has the legal and regulatory capability to combat and prevent money laundering and terrorist financing. The new national anti-money laundering and counterterrorist financing agenda provides the structure for the GOA to improve existing legislation and regulation and enhance interagency coordination. The ongoing challenge is for Argentine law enforcement and regulatory agencies and institutions, including the Ministry of Justice, Central Bank, the UIF, and other institutions to implement fully the National Agenda and aggressively enforce the newly strengthened and expanded legal, regulatory, and administrative measures available to them to combat financial crimes. The GOA could further improve its legal and regulatory structure by enacting

legislation to expand the UIF's role to enable it to investigate money laundering arising from all crimes, rather than just seven enumerated crimes; establishing money laundering as an autonomous offense; and eliminating the current monetary threshold of 50,000 pesos (approximately $16,000) required to establish a money laundering offense. To comply fully with the FATF recommendation on the regulation of bulk money transactions, Argentina should review policy options that are consistent with its MERCOSUR obligations. Other continuing priorities are the effective sanctioning of officials and institutions that fail to comply with the reporting requirements of the law, the pursuit of a training program for all levels of the criminal justice system, and the provision of the necessary resources to the UIF to carry out its mission. There is also a need for increased public awareness of the problem of money laundering and its connection to narcotics, corruption, and terrorism.

Aruba

Aruba is a semi-autonomous constituent part of the Kingdom of the Netherlands; authority over foreign affairs, defense, some judicial functions, human rights, and good governance issue are retained by the Kingdom. Due to its geographic location, casinos, and free trade zones, Aruba is both attractive and vulnerable to narcotics trafficking and money laundering.

Aruba has four commercial and one offshore bank, one mortgage bank, one credit union, an investment bank, a finance company, seven life and general insurance companies, and eleven casinos. The island also has four registered money transmitters, two exempted U.S. money transmitters (Money Gram and Western Union), 13 nonlife and general insurance companies, four captive insurance companies, and 11 company pension funds. There are approximately 5,343 limited liability companies of which 372 are offshore limited liability companies or offshore NVs, which were to have ceased operation in 2008. In addition, there are approximately 2,763 Aruba Exempt Companies (AECs), which mainly serve as vehicles for tax minimization, corporate revenue routing, and asset protection and management.

The offshore NVs and the AECs are the primary methods used for international tax planning in Aruba. The offshore NVs pay a small percentage tax and are subject to more regulation than the AECs. The AECs pay an annual $280 registration fee and must have a minimum of $6,000 in authorized capital. Both offshore NVs and AECs can issue bearer shares. A local managing director is required for offshore NVs. The AECs must have a local registered agent, which must be a trust company.

In 2001, the Government of Aruba (GOA) made a commitment to the Organization for Economic Cooperation and Development (OECD), in connection with the Harmful Tax Practices initiative, to modernize fiscal legislation in line with OECD standards. In 2003, the GOA introduced a New Fiscal Regime (NFR) containing a dividend tax and imputation payment. As of July 1, 2003, the incorporation of low tax offshore NVs was halted. The NFR contains a specific exemption for the AECs. Nevertheless, as a result of commitments to the OECD, the regime was brought in line with OECD standards as of January 2006. As a result of the NFR, Aruba's offshore regime ceased operations by July 1, 2008.

Aruba currently has three designated free zones: Oranjestad Free Zone, Bushiri Free Zone, and the Barcadera Free Zone. The free zones are managed and operated by Free Zone Aruba (FZA) NV, a government limited liability company. Originally, only companies involved in trade or light industrial activities, including servicing, repairing and maintenance of goods with a foreign destination, could be licensed to operate within the free zones. However, State Ordinance Free Zones 2000 extended licensing to service-oriented companies (excluding financial services). Before being admitted to operate in the free zone, companies must submit a business plan along with personal data of managing directors, shareholders, and ultimate beneficiaries, and must establish a limited liability company founded under Aruban law intended exclusively for free zone operations. Aruba took the initiative in the Caribbean Financial Action Task Force (CFATF) to develop regional standards for free zones in

an effort to control trade-based money laundering. The guidelines were adopted at the CFATF Ministerial Meeting in October 2001. Free Zone Aruba NV is continuing the process of implementing and auditing the standards that have been developed.

The Central Bank of Aruba is the supervisory and regulatory authority for banks, insurance companies, company pension funds, and money transfer companies and is responsible for on-site and off-site examinations. However, the Central Bank has not conducted any on-site examinations of its offshore banks. The State Ordinance on the Supervision of Insurance Business (SOSIB) brought all insurance companies under the supervision of the Central Bank. The insurance companies already active before the introduction of this ordinance were also required to obtain a license from the Central Bank. The State Ordinance on the Supervision of Money-Transfer Companies, effective August 2003, places money transfer companies under the supervision of the Central Bank. Quarterly reporting requirements became effective in 2004. A State Ordinance on the supervision of trust companies, which will designate the Central Bank as the supervisory authority, is currently being drafted. Draft legislation to regulate company service providers is also in legislative review.

Aruba's State Ordinance Penalization Money Laundering of 1993 (AB 1993 no. 70) was repealed in 2006 through amendments to the Penal Code (AB 2006 no. 11). The GOA's anti-money laundering legislation extends to all crimes, and the Penal Code allows for conviction-based forfeiture of assets. All financial and nonfinancial institutions, which include banks, money remitters, brokers, insurance companies, and casinos, are obligated to identify clients that conduct transactions over 20,000 Aruban florins $11,300), and report suspicious transactions to Aruba's financial intelligence unit (FIU), the Meldpunt Ongebruikelijke Transacties (MOT). Obligated entities are protected from liability for reporting suspicious transactions. The GOA's anti-money laundering requirements do not extend to such nonfinancial businesses and professions as lawyers, accountants, the real estate sector, or dealers in precious metals and jewels.

The MOT was established in 1996. The MOT is authorized to inspect all obligated entities for compliance with reporting requirements for suspicious transactions and the identification requirements for all financial transactions. The MOT is currently staffed by 10 employees. In 2007, the MOT received approximately 5,715 suspicious transaction reports (STRs) resulting in 180 investigations conducted and 47 cases transferred to the appropriate authorities (statistics for 2008 are not available). The MOT reports that very few STRs are filed by the gaming and insurance sectors.

In June 2000, Aruba enacted a State Ordinance making it a legal requirement to report the cross-border transportation of currency in excess of 20,000 Aruban florins ($11,300) to the Customs Department. The law also applies to express courier mail services. Reports generated are forwarded to the MOT to review, and in 2007, approximately 820 such reports were submitted.

The MOT shares information with other national government departments. In April 2003, the MOT signed an information exchange agreement with the Aruba Tax Office, which is in effect and being implemented. The MOT and the Central Bank have also signed an information exchange memorandum of understanding (MOU), effective January 2006. The MOT is not linked electronically to the police or prosecutor's office. The MOT is a member of the Egmont Group and is authorized by law to share information with members of the Egmont Group through MOUs.

In 2004, the Penal Code of Aruba was modified to criminalize terrorism, the financing of terrorism, and related criminal acts. The GOA has a local committee comprised of officials from different departments of the Aruban Government, under the leadership of the MOT, to oversee the implementation of Financial Action Task Force (FATF) Forty Recommendations on Money Laundering and Nine Special Recommendations on Terrorist Financing. The local committee, FATF Committee Aruba, reviewed the GOA anti-money laundering legislation and proposed, in accordance with the FATF Nine Special Recommendations on Terrorist Financing, amendments to existing legislation and introduction of new laws. In 2007, the Parliament of Aruba approved the Ordinance on

Sanctions 2006 (AB 2007 no. 24), to enhance the GOA's compliance with the FATF Special Recommendations. The GOA and the Netherlands formed a separate committee in 2004 to ensure cooperation of agencies within the Kingdom of the Netherlands in the fight against cross-border organized crime and international terrorism.

The bilateral agreement between the Kingdom of the Netherlands (KON) and the United States Government (USG) regarding mutual cooperation in the tracing, freezing, seizure, and forfeiture of proceeds and instrumentalities of crime and the sharing of forfeited assets, which entered into force in 1994, applies to Aruba. The Mutual Legal Assistance Treaty between the KON and the USG also applies to Aruba, though it is not applicable to requests for assistance relating to fiscal offenses addressed to Aruba. The Tax Information Exchange Agreement with the United States, signed in November 2003, became effective in September 2004.

The KON extended application of the 1988 UN Drug Convention to Aruba in 1999, the UN International Convention for the Suppression of the Financing of Terrorism in 2005, and the UN Convention against Transnational Organized Crime in 2007. The Kingdom has not yet extended application of the UN Convention against Corruption to Aruba. Aruba participates in the Financial Action Task Force (FATF) as part of the Kingdom of the Netherlands and underwent a mutual evaluation in November 2008. The GOA is also a member of CFATF. The MOT became a member of the Egmont Group in 1997. Aruba is also a member of the Offshore Group of Banking Supervisors.

The Government of Aruba has shown a commitment to combating money laundering and terrorist financing by establishing an anti-money laundering and counterterrorist financing regime that is generally consistent with the recommendations of the FATF and CFATF. Aruba should take additional steps to immobilize bearer shares under its fiscal framework and to enact its long-pending ordinance addressing the supervision of trust companies. The GOA should ensure that all obligated entities are fully complying with their anti-money laundering and counterterrorist financing reporting requirements, and consider extending these reporting requirements to designated nonfinancial businesses and professions.

Australia

Australia is one of the major centers for capital markets in the Asia-Pacific region. In 2006-07, turnover across Australia's over-the-counter and exchange-traded financial markets was AU $120 trillion (approximately $78 trillion). Australia's total stock market capitalization is over AU $1.63 trillion (approximately $1.1 trillion), making it the eighth largest market in the world, and the third largest in the Asia-Pacific region behind Japan and Hong Kong. Australia's foreign exchange market is ranked seventh in the world by turnover, with the U.S. dollar and the Australian dollar the fourth most actively traded currency pair globally. While narcotics offences provide a substantial source of proceeds of crime, the majority of illegal proceeds are derived from fraud-related offences. A 2004 Australian Government estimate suggests that the amount of money laundered in Australia is in the vicinity of AU $4.5 billion (approximately $ 3 billion) per year.

The Government of Australia (GOA) has maintained a comprehensive system to detect, prevent, and prosecute money laundering. The last five years have seen a noticeable increase in activities investigated by Australian law enforcement agencies that relate directly to offenses committed overseas. Australia's system has evolved over time to address new money laundering and terrorist financing risks identified through continuous consultation between government agencies and the private sector.

Subsequent to the Financial Action Task Force (FATF) Mutual Evaluation, the GOA has committed to reforming Australia's AML/CTF system to implement the revised FATF Forty plus Nine recommendations. The Attorney General's Department (AGD) is coordinating this process, now

underway, which is significantly reshaping Australia's AML/CTF regime and bringing it into line with current international best practices.

Australia criminalized money laundering related to serious crimes with the enactment of the Proceeds of Crime Act 1987. This legislation also contained provisions to assist investigations and prosecution in the form of production orders, search warrants, and monitoring orders. It was superseded by two acts that came into force on January 1, 2003 (although proceedings that began prior to that date under the 1987 law will continue under that law). The Proceeds of Crime Act 2002 provides for civil forfeiture of proceeds of crime as well as for continuing and strengthening the existing conviction-based forfeiture scheme that was in the Proceeds of Crime Act 1987. The Proceeds of Crime Act 2002 also enables freezing and confiscation of property used in, intended to be used in, or derived from, terrorism offenses. It is intended to implement obligations under the UN Convention for the Suppression of the Financing of Terrorism and resolutions of the UN Security Council relevant to the seizure of terrorism-related property. The Act also provides for forfeiture of literary proceeds where these have been derived from commercial exploitation of notoriety gained from committing a criminal offense.

The Proceeds of Crime (Consequential Amendments and Transitional Provisions) Act 2002 (POCA 2002), repealed the money laundering offenses that had previously been in the Proceeds of Crime Act 1987 and replaced them with updated offenses that have been inserted into the Criminal Code. The new offenses in Division 400 of the Criminal Code specifically relate to money laundering and are graded according both to the level of knowledge required of the offender and the value of the property involved in the activity constituting the laundering. As a matter of policy all very serious offenses are now gradually being placed in the Criminal Code. POCA 2002 also enables the prosecutor to apply for the restraint and forfeiture of property from proceeds of crime. POCA 2002 further creates a national confiscated assets account from which, among other things, various law enforcement and crime prevention programs may be funded. Recovered proceeds can be transferred to other governments through equitable sharing arrangements.

The Anti-Money Laundering and Counter-Terrorism Financing Act (AML/CTF Act) received Royal Assent on December 12, 2006 and was subsequently amended on April 12, 2007. The Act forms part of a legislative package that implements the first tranche of reforms to Australia's AML/CTF regulatory regime. The AML/CTF Act covers the financial sector, gambling sector, bullion dealers and any other professionals or businesses that provide particular 'designated services'. The Act imposes a number of obligations on entities that provide designated services, including customer due diligence, reporting obligations, record keeping obligations, and the requirement to establish and maintain an AML/CTF program. The AML/CTF Act implements a risk-based approach to regulation and the various obligations under the Act will be implemented over a two-year period. The legislative framework authorizes operational details to be settled in AML/CTF Rules, which will be developed by the Australian Transaction Reports and Analysis Centre (AUSTRAC) in consultation with industry. During 2007-08, AUSTRAC published 11 Rules relating to the AML/CTF Act, all developed in consultation with industry. AUSTRAC has also published a number of guidance notes for entities, including guidance regarding correspondent banking and providers of designated remittance services.

A requirement went into effect for reporting entities to submit an AML/CTF compliance report to AUSTRAC indicating their level of preparedness and compliance with AML/CTF rules, in March 2008. An AML/CTF compliance report provides information about reporting entities' compliance with the AML/CTF Act 2006, the regulations and the AML/CTF Rules. It is required under the AML/CTF Act in Part 3, Division 5, which came into effect in June 2007. The compliance reports provide AUSTRAC and the reporting entity an indication of their progress in implementing their AML/CTF obligations.

The Australian Government is working on a second tranche of AML/CTF reforms, which will extend regulatory obligations to designated services provided by real estate agents, dealers in precious stones and metals, and specified legal, accounting, trust and company services (lawyers and accountants were included in the first tranche, but only where they compete with the financial sector and not for general services). The AGD has actively engaged with a broad cross-section of entities and interest groups regarding the proposed reforms.

The AML/CTF Act will gradually replace the Financial Transaction Reports Act 1988 (FTR Act) which currently operates concurrently to the AML/CTF Act. As a result of the passage of the AML/CTF (Transitional Provisions and Consequential Amendments) Act, a number of amendments to other Commonwealth legislation, including the FTR Act, were necessary. The AML/CTF Act makes those amendments, which include the repeal of some provisions of the FTR Act. The second tranche includes further obligations in relation to customer due diligence and reporting, commenced in December 2008.

The FTR Act was enacted to combat tax evasion, money laundering, and serious crimes and it requires banks and nonbanking financial entities (collectively referred to as cash dealers) to verify the identities of all account holders and signatories to accounts, and to retain the identification record, or a copy of it, for seven years after the day on which the relevant account is closed. A cash dealer, or an officer, employee, or agent of a cash dealer, is protected against any action, suit, or proceeding in relation to the reporting process. The FTR Act also establishes reporting requirements for Australia's cash dealers. Required to be reported are: suspicious transactions, cash transactions equal to or in excess of AU $10,000 (approximately U.S. $6,500), and all international funds transfers into or out of Australia, regardless of value. The FTR Act will continue to apply to cash dealers who are not reporting entities under the AML/CTF Act.

FTR Act reporting also applies to nonbank financial institutions such as money exchangers, money remitters, stockbrokers, casinos and other gambling institutions, bookmakers, insurance companies, insurance intermediaries, finance companies, finance intermediaries, trustees or managers of unit trusts, issuers, sellers, and redeemers of travelers checks, bullion sellers, and other financial services licensees. Solicitors (lawyers) are also required to report significant cash transactions. Accountants do not have any FTR Act obligations. However, they do have an obligation under a self-regulatory industry standard not to be involved in money laundering transactions.

AUSTRAC was established under the FTR Act and is continued in existence by the AML/CTF Act. AUSTRAC is Australia's AML/CTF regulator and specialist financial intelligence unit (FIU). AUSTRAC collects, retains, compiles, analyzes, and disseminates financial transaction report (FTR) information. AUSTRAC also provides advice and assistance to revenue collection, social justice, national security, and law enforcement agencies, and issues guidelines to regulated entities regarding their obligations under the FTR Act, AML/CTF Act and the Regulations and Rules. Under the AML/CTF Act, AUSTRAC is the national AML/CTF regulator with supervisory, monitoring and enforcement functions over a diverse range of business sectors. As such, AUSTRAC plays a central role in Australia's AML system both domestically and internationally. During the 2007-08 Australian financial year, AUSTRAC's FTR information was used in 2968 operational matters. Results from the Australian Taxation Office (ATO) shows that the FTR information contributed to more than AU $76 million (approximately U.S. $49 million) in ATO assessments during the year. In 2007-08, AUSTRAC received 17,965,373 financial transaction reports, with 99.7 percent of the reports submitted electronically through the EDDS Web reporting system. AUSTRAC received 29,089 suspect transaction reports (SUSTRs), an increase of 19 percent over the previous year.

During 2007-08, there was a significant increase in the total number of financial transaction reports received by AUSTRAC. Significant cash transactions reports (SCTRs) account for 16 percent of the total number of FTRs reported to AUSTRAC in 2007-08 and are reported by cash dealers and

solicitors. In 2007-08, AUSTRAC received 2.934,855 SCTRs, an increase of 9.7 percent from the previous year. Cash dealers are also required to report all international funds transfer instructions (IFTIs) to AUSTRAC. Cash dealers reported 14,963,719 IFTIs to AUSTRAC during the financial year—a 15.0 percent increase from 2005-06. Cross-border movement of physical currency (CBM-PC) reports (which have replaced international currency transfer reports, ICTRs) are primarily declared to the Australian Customs Service (ACS) by individuals when they enter or depart from Australia. For 2007-08, AUSTRAC received 36,131 CPM-PC reports, a 54.7 percent decrease from the previous financial year. This increase in reports came after AUSTRAC and ACS undertook extensive public awareness campaigns during 2007-08 to inform travelers of their obligation to declare physical currency. The Infringement Notice Scheme (INS) is a penalty-based scheme introduced in 2007 under the AML/CTF Act to strengthen Australia's cross border movement procedures. An ACS or Australian Federal Police (AFP) officer can issue infringements at the border where there is a failure to report a cross border movement of physical currency (CBM-PC) or the cross border movement of a bearer negotiable instrument (CBM-BNI; for example, travelers checks). The issuing of infringements for a failure to report a CBM-BNI is based on disclosure upon request rather than a declaration.

In April 2005, the Minister for Justice and Customs launched AUSTRAC's AML eLearning application. This application has been well received by cash dealers as a tool in providing basic education on the process of money laundering, the financing of terrorism, and the role of AUSTRAC in identifying and assisting investigations of these crimes. In December 2007, the Minister for Home Affairs launched three new tools to assist industry compliance with AML/CTF obligations, in addition to updating the eLearning application. AUSTRAC Online is a secure Internet-based system that assists entities adhere to their reporting and regulatory obligations, and enables them to access their own information. The AUSTRAC Regulatory Guide is an instructional and 'living' document that assists industry to understand and meet their AML/CTF obligations, which will be updated as further AML/CTF Act provisions are implemented. Lastly, the AUSTRAC Typologies and Case Studies Report 2007 was published to raise industry awareness regarding potential AML/CTF risk factors, methods and typologies.

The Australian Prudential Regulation Authority (APRA) is the prudential supervisor of Australia's financial services sector. AUSTRAC regulates anti-money laundering/counterterrorist financing (AML/CTF) compliance. The FATFME noted that a comprehensive system for AML/CTF compliance for the entire financial sector needed to be established by the GOA, as does an administrative penalty regime for AML/CTF noncompliance. As a result, the AML/CTF Act has given AUSTRAC a wide range of enhanced enforcement powers to complement the criminal sanctions that were available under the FTR Act. The AML/CTF Act provides AUSTRAC with a civil penalty framework and other intermediate sanctions, such as enforceable undertakings, remedial directions and external audits for noncompliance. AUSTRAC places a great deal of emphasis on educating and continuously engaging the private sector regarding the evolution of AML/CTF regime and the attendant reporting requirements. Between July 2007 and July 2008, AUSTRAC delivered more than 215 education sessions to approximately 5000 people from more than 1500 reporting entities ranging from banks and mortgage brokers, to pubs and casinos and designated remittance services. Additionally, AUSTRAC provided more than 100 presentations to partner agencies, including the Australian Federal Police (AFP), the Customs Service, Taxation Office and the State and Territory Police. In 2007-08 AUSTRAC developed and began implementation of a new on-site assessment strategy, including governance arrangements, a target for the number of annual inspections to be done, and inspection selection criteria. AUSTRAC in 2007-08 conducted over 130 on-site assessments of reporting entities to assess their compliance with FTR Act and AML/CTF Act obligations.

In June 2002, Australia passed the Suppression of the Financing of Terrorism Act 2002 (SFT Act). The aim of the SFT Act is to restrict the financial resources available to support the activities of terrorist organizations. It criminalizes terrorist financing and substantially increases the penalties that

apply when a person uses or deals with suspected terrorist assets that are subject to freezing. The SFT Act enhances the collection and use of financial intelligence by requiring cash dealers to report suspected terrorist financing transactions to AUSTRAC, and relaxes restrictions on information sharing with relevant authorities regarding the aforementioned transactions. The SFT Act also addresses commitments Australia has made with regard to the UNSCR 1373 and is intended to implement the UN International Convention for the Suppression of the Financing of Terrorism. Under this Act three accounts related to an entity listed on the UNSCR 1267 Sanction Committee's consolidated list, the International Sikh Youth Federation, were frozen in September 2002. While there have been some charges laid for acts in preparation of terrorism, there have been no terrorist financing charges or prosecutions under this legislation. The Security Legislation Amendment (Terrorism) Act 2002 also inserted new criminal offenses in the Criminal Code for receiving funds from, or making funds available to, a terrorist organization.

The Anti-Terrorism Act (No.2) 2005 (AT Act), which took effect on December 14, 2006, amends offenses related to the funding of a terrorist organization in the Criminal Code so that they also cover the collection of funds for or on behalf of a terrorist organization. The AT Act also inserts a new offense of financing a terrorist. The AML/CTF Act further addressed terrorist financing by placing an obligation on providers of designated remittance services to register with AUSTRAC.

The Australian Government is also developing a strategy for improving controls to prevent the misuse of non profit organizations (NPOs) for financing terrorism. A critical aspect of this strategy will be to work in partnership with the NPO sector to raise awareness about the vulnerability of the sector to abuse for terrorism financing. A review is underway to determine if any gaps exist in information currently collected from the NPO sector by Australian government agencies.

Investigations of money laundering reside with the AFP and Australian Crime Commission (Australia's only national multi-jurisdictional law enforcement agency). The AFP is the primary law enforcement agency for the investigation of money-laundering and terrorist-financing offences in Australia at the Commonwealth level and has both a dedicated Financial Crimes Unit and well staffed Financial Investigative Teams (FIT) with primary responsibility for asset identification/restraint and forfeiture under the POCA 2002. The Commonwealth Director of Public Prosecutions (CDPP) prosecutes offences against Commonwealth law and to recover proceeds of Commonwealth crime. The main cases prosecuted by the CDPP involve drug importation and money laundering offences. The Australian Federal Police accepted 52 new money laundering investigations from July 2007 to April 2008 and restrained AU $37,831,143 (approximately U.S. $24,630,000) of which AU $341,923 (approximately $6,082,000) was forfeited. From July 2007 through mid-May 2008, the CDPP reported that 68 indictments for money laundering were issued. At the July 2008 plenary of Asia Pacific Group held in Bali, Indonesia, Australian delegation mentioned that a conviction for money laundering involving AU $43,000 (approximately $30,000) was the largest sum ever involved in a successfully prosecuted money laundering case in the country. In April 2003, the AFP established a Counter Terrorism Division to undertake intelligence-led investigations to prevent and disrupt terrorist acts. A number of Joint Counter Terrorism Teams (JCTT), including investigators and analysts with financial investigation skills and experience, are conducting investigations specifically into suspected terrorist financing in Australia. The AFP also works closely with overseas counterparts in the investigation of terrorist financing, and has worked closely with the FBI on matters relating to terrorist financing structures in South East Asia. In 2006, AFP introduced mandatory consideration of potential money laundering and crime proceeds into its case management processes, thereby ensuring that case officers explore the possibility of money laundering and crime proceeds actions in all investigations conducted by the AFP.

The GOA participates in the Strategic Alliance Group. This group of five countries includes representatives from the UK Serious Organized Crime Agency (SOCA), the Royal Canadian Mounted Police (RCMP), the Australian Federal Police (AFP), the New Zealand Police (NZP), the United

States Immigration and Customs Enforcement (ICE), the Drug Enforcement Administration (DEA), and the Federal Bureau of Investigation (FBI), all of whom analyze various genres of criminal activity and exchange information and best practices.

Australia is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime and its protocol on migrant smuggling. In September 1999, a Mutual Legal Assistance Treaty between Australia and the United States entered into force. Australia participates actively in a range of international fora, including the FATF, the Pacific Islands Forum, and the Commonwealth Secretariat. Through its funding and hosting of the Secretariat of the Asia/Pacific Group on Money Laundering (APG), of which it serves as permanent co-chair, the GOA has elevated money laundering and terrorist financing issues to a priority concern among countries in the Asia/Pacific region. AUSTRAC is an active member of the Egmont Group of Financial Intelligence Units (FIUs); AUSTRAC's CEO was appointed to a one-year term as Chair of the Egmont Commission in May 2008. AUSTRAC has signed Exchange Instruments, mostly in the form of Memoranda of Understanding (MOUs) allowing the exchange of financial intelligence, with FinCEN and the FIUs of 52 other countries. AUSTRAC has also signed 34 domestic MOUs with Commonwealth, State, and Territory partner agencies covering a spectrum of agencies to include regulatory, law enforcement, social justice, national security and revenue.

Following the bombings in Bali in October 2002, the Australian Government announced an AU $10 million (approximately $6.5 million) initiative managed by the Australian Agency for International Development (AusAID), to assist in the development of counterterrorism capabilities in Indonesia. As part of this initiative, the AFP has established a number of training centers such as the Jakarta Centre for Law Enforcement Cooperation. AUSTRAC, ACS and the AFP worked closely with agencies from the United States and Japan to hold the South-East Asian Regional Bulk Cash Smuggling Workshop at the Jakarta Centre for Law Enforcement Cooperation (JCLEC) in Semarang, Indonesia in April 2008. As part of Australia's broader regional assistance initiatives, AUSTRAC has continued its South East Asia Counter Terrorism Program of providing capacity building assistance to 10 South East Asian nations, to develop capacity in detecting and dealing with terrorist financing and money laundering; this program will continue until 2009-10. AUSTRAC assisted the Indonesian FIU, PPATK (Indonesian Financial Transaction Reports and Analysis Center), in developing a program for the receipt and analysis of suspicious transaction reports and the improvement of data quality and information processing. In the Pacific region, AUSTRAC has developed and provided unique software ("FIU-in-a-Box") and training for personnel to six Pacific island FIUs (Cook Islands, Solomon Islands, Samoa, Tonga, Palau and Vanuatu) to fulfill their domestic obligations and share information with foreign analogs, and conducted a review of these FIUs in June 2008. AUSTRAC concluded IT Needs Assessments in Papua New Guinea and Nauru in 2007-08 as part of its engagement with Pacific FIUs. The AGD received a grant of AU $7.7 million (approximately U.S. $5.1 million) over four years to establish the Anti-Money Laundering Assistance Team (AMLAT). AMLAT works cooperatively with the U.S. Department of State-funded Pacific Islands Anti-Money Laundering Program (PALP) to enhance AML/CTF regimes for Pacific island jurisdictions. The PALP, a four-year program, is managed by the United Nations Global Program against Money Laundering and employs residential and intermittent mentors to develop or enhance existing AML/CTF regimes in the non-FATF member states of the Pacific Islands Forum.

The GOA continues to pursue a comprehensive anti-money laundering/counterterrorist financing regime that meets the objectives of the revised FATF Forty Recommendations and Nine Special Recommendations on Terrorist Financing. To enhance its AML/CTF regime, as noted in the FATF mutual evaluation, AUSTRAC has been provided with substantially increased powers to ensure compliance. There will be more on-site compliance audits and AUSTRAC can require regular compliance reports from reporting entities; can initiate monitoring orders and statutory demands for

information and documents; can seek civil penalty orders, remedial directions and injunctions; and, can require a reporting entity to subject itself to an external audit of its AML/CTF program. The AML/CTF Act also provides for greater coordination amongst the regulatory agencies of its financial, securities and insurance sectors.

The GOA is continuing its exemplary leadership role in emphasizing money laundering/terrorist finance issues and trends within the Asia/Pacific region and its commitment to providing training and technical assistance to the jurisdictions in that region. Having significantly enhanced its increased focus on AML/CTF deterrence, the Government of Australia should increase its efforts to prosecute and convict money launderers.

Austria

Austria is a major financial center, and Austrian banking groups control significant shares of the banking markets in Central, Eastern and Southeastern Europe. According to Austrian National Bank statistics, Austria ranks among those with the highest numbers of banks and bank branches per capita in the world, with 870 banks and one bank branch for every 1,610 people. Austria is not an offshore jurisdiction. Money laundering occurs within the Austrian banking system as well as in nonbank financial institutions and businesses. The volume of undetected organized crime may be enormous, with much of it reportedly coming from the former Soviet Union. Money laundered by organized crime groups derives primarily from serious fraud, corruption, narcotics-trafficking and trafficking in persons. Criminal groups use various instruments to launder money, including informal money transfer systems, the Internet, and offshore companies.

Austria criminalized money laundering in 1993. Predicate offenses include terrorist financing and other serious crimes. The law is stricter for money laundering by criminal organizations and terrorist "groupings," because in such cases the law requires no proof that the money stems directly or indirectly from prior offenses. Since January 1, 2008, the GOA has implemented strict new criminal regulations against corruption that define corruption as an additional predicate offense, and has appointed a special public prosecutor with responsibility for corruption investigations and indictments in all of Austria.

The Law on Responsibility of Associations mandates criminal responsibility for all legal entities, general and limited commercial partnerships, registered partnerships and European Economic Interest Groupings, but not charitable or nonprofit entities. The law covers all crimes listed in the Criminal Code, including corruption, money laundering and terrorist financing.

Amendments to the Customs Procedures Act and the Tax Crimes Act of 2004 and 2006 address the problem of cash couriers and international transportation of currency and monetary instruments from illicit sources. Austrian customs authorities do not automatically screen all persons entering Austria for cash or monetary instruments. However, to implement the European Union (EU) regulation on controls of cash entering or leaving the EU, the Government of Austria (GOA) requires an oral or written declaration for cash amounts of 10,000 euros (approximately $14,300) or more. This declaration, which includes information on source and use, must be provided when crossing an external EU border. Spot checks for currency at border crossings and on Austrian territory do occur. Customs officials have the authority to seize suspect cash, and will file a report with the Austrian financial intelligence unit (FIU) in cases of suspected money laundering. Austria has no database for cash smuggling reports.

The Banking Act of 1994 creates customer identification, record keeping, and staff training obligations for the financial sector. Entities subject to the Banking Act include banks, leasing and exchange businesses, safe custody services, and portfolio advisers. The law requires financial institutions to identify all customers when beginning an ongoing business relationship. In addition, the

Banking Act requires customer identification for all transactions of more than 15,000 euros (approximately $21,450) for customers without a permanent business relationship with the bank. Identification procedures require that all customers appear in person and present an official photo identification card. These procedures also apply to trustees of accounts, who must disclose the identity of the account beneficiary. Procedures allow customers to carry out non-face-to-face transactions, including Internet banking, on the basis of a secure electronic signature or a copy of a picture ID and a legal business declaration submitted by registered mail.

An amendment to the Banking Act, in effect since January 1, 2008, tightens customer identification procedures by requiring renewed identification in case of doubt about previously obtained ID documents or data, as well as requiring personal appearances of trustees. Regulations also require institutions to determine the identity of beneficial owners and introduce risk-based customer analysis for all customers. Financial institutions must also implement these requirements in their subsidiaries abroad. The 2008 Banking Act amendment also broadens the reporting requirement by replacing "well-founded suspicion" with "suspicion or probable reason to assume" that a transaction serves the purpose of money laundering or terrorist financing or that a customer has violated his duty to disclose trustee relationships.

Enhanced due diligence obligations apply if the customer has not been physically present for identification purposes (for example, non-face-to-face transactions or Internet banking), and with regard to cross-border correspondent banking relationships. In cases where a financial institution is unable to establish customer identity or obtain other required information on the business relationship, it must decline to enter into a business relationship or process a transaction, or terminate the business relationship. The institution must consider reporting the case to the FIU. The law also requires financial institutions to keep records on customers and account owners. The Securities Supervision Act of 1996, which covers trade of securities, shares, money market instruments, options, and other instruments listed on an Austrian stock exchange or any regulated market in the EU, refers to the Banking Act's identification regulations. The Insurance Act of 1997 includes similar regulations for insurance companies underwriting life policies. An amendment to the Insurance Act of 1997, in effect since January 1, 2008, tightens record keeping requirements for insurance companies.

The law holds individual bankers responsible if their institutions launder money. The Banking Act and other laws provide "safe harbor" to obligated reporting individuals, including bankers, auctioneers, real estate agents, lawyers, and notaries. The law excuses those who report from liability for damage claims resulting from delays in completing suspicious transactions. Although there is no requirement for banks to report large currency transactions unless they are suspicious, the FIU provides outreach and information to banks to raise awareness of large cash transactions.

On January 1, 2008, responsibility for on-site inspections of banks, exchange businesses and money transmitters moved from the Financial Market Authority (FMA) to the Austrian National Bank. These on-site inspections, including inspections at subsidiaries abroad, are all-inclusive, and require analysis of financial flows and compliance with money laundering regulations. Money remittance businesses require a banking license from the FMA and are subject to supervision. Informal remittance systems, such as hawala, exist in Austria but are subject to administrative fines for carrying out banking business without a license. On its website, the FMA has published several circular letters with details on customer identification, money laundering and terrorist financing regulations, and reporting of suspicious transactions.

The Austrian Gambling Act, the Business Code, and the Austrian laws governing lawyers, notaries, and accounting professionals introduce additional money laundering and terrorist financing regulations concerning customer identification, reporting of suspicious transaction reports (STRs) and record keeping for dealers in high value goods, auctioneers, real estate agents, casinos, lawyers, notaries, certified public accountants, and auditors. Amendments to the Stock Exchange Act, the Securities

Supervision Act, the Insurance Act, and Austrian laws governing lawyers and notaries came into effect on January 1, 2008. The amendment to the Gambling Act has been in effect since August 26, 2008, and the amendment to the law governing accounting professionals since April 23, 2008. These introduced stricter regulations regarding customer identification procedures, including requiring customer identification for all transactions of more than 15,000 euros (approximately $21,450) for customers without a permanent business relationship. Lawyers and notaries are exempt from their reporting obligations for information obtained in the course of judicial proceedings or providing legal advice to a client unless the client has sought legal advice for laundering money or financing terrorism. The Business Code amendment requires all traders, not only dealers in high-value goods, auctioneers and real estate agents, to establish the identity of customers for cash transactions of 15,000 euros (approximately $21,450) or more.

The EU regulation on wire transfers (EC 1781/2006) entered into force on January 1, 2007, and became immediately and directly applicable in Austria. Since January 1, 2007, financial institutions require customer identification for all fund transfers of 1,000 euros (approximately $1,430) or more.

Austria's FIU is located within the Austrian Interior Ministry's Bundeskriminalamt (Federal Criminal Intelligence Service). The FIU is the central repository of STRs and has police powers. During the first ten months of 2008, the FIU received approximately 910 STRs from banks and others—a figure indicating little change from the 1,085 suspicious transactions reported in 2007. The FIU has also responded to requests for information from Interpol, Europol, other FIUs, and other authorities. There were ten money laundering convictions in 2006 and 18 in 2007.

Since 1996, legislation has provided for asset seizure and the forfeiture of illegal proceeds. The banking sector generally cooperates with law enforcement efforts to trace funds and seize illicit assets. Austria has regulations in the Code of Criminal Procedure that are similar to civil forfeiture in the U.S. In connection with money laundering, organized crime and terrorist financing, all assets are subject to seizure and forfeiture, including bank assets, other financial assets, cars, legitimate businesses, and real estate. Courts may freeze assets in the early stages of an investigation. In the first ten months of 2008, Austrian courts froze assets worth more than 110 million euros (approximately $157,000,000).

The Extradition and Judicial Assistance Law provides for expedited extradition; expanded judicial assistance; acceptance of foreign investigative findings in the course of criminal investigations; and enforcement of foreign court decisions. Austria's strict bank secrecy regulations can be lifted in cases of suspected money laundering. Moreover, bank secrecy does not apply in cases in which banks and other financial institutions must report suspected money laundering.

The 2002 Criminal Code Amendment introduces the following criminal offense categories: terrorist "grouping," terrorist criminal activities, and financing of terrorism, in line with UNSCR 1373. The Criminal Code defines "financing of terrorism" as a separate criminal offense category, punishable in its own right. Terrorist financing is also included in the list of criminal offenses subject to domestic jurisdiction and punishment, regardless of the laws where the act occurred. The money laundering offense is also expanded to terrorist "groupings." The Federal Economic Chamber's Banking and Insurance Department, in cooperation with all banking and insurance associations, has published an official Declaration of the Austrian Banking and Insurance Industries to Prevent Financial Transactions in Connection with Terrorism. The law also gives the judicial system the authority to identify, freeze, and seize terrorist financial assets. Asset forfeiture regulations cover funds collected or held available for terrorist financing, and permit freezing and forfeiture of all assets that are in Austria, regardless of whether the crime was committed in Austria or the whereabouts of the criminal.

The Austrian authorities distribute to all financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list, as well as the list of Specially Designated Global Terrorists that the United States has designated pursuant to Executive Order 13224, and those distributed by the EU to members. According to the Ministry of

Justice and the FIU, no accounts found in Austria have shown any links to terrorist financing. The FIU immediately shares all reports on suspected terrorist financing (35 in 2007 and 26 during the first ten months of 2008) with the Austrian Interior Ministry's Federal Agency for State Protection and Counterterrorism (BVT). There were no convictions for terrorist financing in 2006 or 2007.

The GOA has undertaken important efforts that may help thwart the misuse of charitable or nonprofit entities as conduits for terrorist financing. The Law on Associations covers charities and all other nonprofit associations in Austria. The law regulates the establishment of associations, by-laws, organization, management, association registers, appointment of auditors, and detailed accounting requirements. Since January 1, 2007, associations whose finances exceed a certain threshold are subject to special provisions. Each association must appoint two independent auditors and must inform its members about its finances and the auditor's report. Associations with a balance sheet exceeding 3 million euros (approximately $4,300,000) or annual donations of more than 1 million euros (approximately $1,430,000) must appoint independent auditors to review and certify the financial statements. Public collection of donations requires advance permission from the authorities. The Central Register of Associations offers basic information on all registered associations in Austria free of charge via the Internet. Stricter customer identification procedures and due diligence obligations for financial institutions will implement an additional layer of monitoring for charities and nonprofit organizations, particularly in cases where business relationships suggest they could be connected to money laundering or terrorist financing.

The GOA is generally cooperative with U.S. authorities in money laundering cases. Austria has not enacted legislation that provides for sharing forfeited narcotics-related assets with other governments. However, a bilateral U.S.—GOA agreement on sharing of forfeited assets is pending signature in both the U.S. and Austria. In addition to the exchange of information with home country supervisors permitted by the EU, Austria has defined this information exchange in agreements with more than a dozen other EU members and with Croatia.

Austria is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. Austria is a member of the FATF and will undergo a FATF mutual evaluation in 2009. The FIU is a member of the Egmont Group.

The Government of Austria has implemented a viable, comprehensive anti-money laundering and counterterrorist financing regime. The GOA should ensure it provides the FIU and law enforcement the resources they require to effectively perform their functions. The GOA should introduce safe harbor legislation protecting FIU and other government personnel from damage claims as a result of their work. Customs authorities should continue spot-checking operations for bulk cash smuggling despite the lack of border controls with Austria's neighbors. The GOA should consider mandating the reporting of all currency transactions exceeding an established threshold. The GOA also should consider enacting legislation that will provide for asset sharing with other governments.

Azerbaijan

The following information was obtained primarily from the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) public statement of December 12, 2008 and the mutual evaluation report on Azerbaijan adopted at the MONEYVAL plenary in December 2008.

At the crossroads of Europe and Central Asia and with vast amounts of natural resources, Azerbaijan is a rapidly growing economy. The illicit drug trade generates the largest amount of illicit funds by far, followed by theft and fraud. Illicit funds also derive from robbery, tax evasion, and smuggling, and in recent years, trafficking in persons has also become an increasing problem that generates illicit funds.

Corruption is endemic in the country, and organized crime groups exist as well, although authorities do not have a good understanding of the groups or their operations. Azerbaijani authorities believe that money laundering and terrorist financing operates largely through the banking sector.

Economic growth, fueled by the oil and natural gas resources present in Azerbaijan and the energy sector, is strong. International trade has also been increasing since independence, as has foreign investment. At the end of 2007, Azerbaijan had 46 commercial banks, 6 of which worked mostly with foreign capital. Two banks are completely state-owned. There were 77 licensed credit unions and 18 licensed microfinance institutions, as well as 29 licensed insurance companies. As of January 1, 2008, Azerbaijan had 37 licensed professional securities actors.

Azerbaijan's Customs authorities have received no guidance regarding identification of potential money launderers or terrorist financiers entering or exiting the country. Even if Customs suspected financial crime, the agency does not have the legal authority to interdict or confiscate currency, nor does it have the obligation to report suspicions to other law enforcement authorities.

In 2003, law enforcement found a number of charitable organizations linked to terrorist financing and shut them down. Authorities remain cognizant of the vulnerabilities that the nonprofit sector poses and consider nonprofit organizations (NPOs) reporting entities. However, Azerbaijan has not examined the risks of this sector and authorities have not reviewed the organizations for terrorist financing vulnerabilities.

In February 2006 MONEYVAL initiated Compliance Enhancing Procedures against Azerbaijan due to its failure to pass satisfactory and comprehensive AML/CTF preventive legislation, lack of an FIU and lack of a legally based and effective STR regime. In February 2008, MONEYVAL conducted a high-level visit to draw the attention of senior Azerbaijani authorities to the importance of an anti-money laundering/counterterrorist financing (AML/CTF) regime. In April 2008, MONEYVAL assessors conducted an on-site evaluation of the Azerbaijan AML/CTF regime, which the plenary adopted in December 2008. In December 2008, MONEYVAL issued a public statement registering its concern with Azerbaijan's failure to pass and implement an AML/CTF law, and calling upon member states and other countries to advise their financial institutions to apply enhanced due diligence to transactions with links to Azerbaijan.

The Government of Azerbaijan (GOAJ) has no AML/CTF preventative law in place, although a draft law passed a second reading on October 31, 2008. Reportedly, when implemented, the draft law anti-money law will, in part, address some of the current shortcomings, such as anonymous accounts, enhanced due diligence for politically exposed persons (PEPs), freezing and seizure protocols and the filing of suspicious transaction reports, although the draft law does not comport with international standards. The GOAJ has recently advised that it intends to amend the draft law to meet international standards. The GOAJ has instituted some provisions aimed at criminalizing money laundering, but the current provisions in place designed to criminalize money laundering have major deficiencies and there has been no implementation. Only natural persons are subject to criminal liability for money laundering. Azerbaijan has not applied the principles of corporate criminal liability, so no legal persons can be punished for money laundering or terrorist financing. Azerbaijan has taken the "all crimes" approach to predicate offenses. However, insider trading and market manipulation are not considered offenses.

The mutual evaluation report (MER) noted that the GOAJ provided no evidence of investigations or court proceedings involving money laundering as a stand-alone offense. Under the current patchwork regime, it is unclear whether prosecutors must obtain a conviction for the predicate offense in order to open a money laundering investigation. It is also unclear whether authorities can pursue money laundering if the predicate offense takes place in another country. Azerbaijan has no criminal liability for legal persons. Only natural persons can receive punishment for money laundering and terrorist financing.

Although in the absence of a comprehensive law there are no specific supervisory bodies for AML/CTF compliance in the various sectors, authorities maintain that the AML/CTF competencies are addressed by the supervisors in the course of general supervisory activities. The National Bank of Azerbaijan (NBA) is the supervisory authority for banks and credit unions. The Ministry of Finance supervises insurance companies, and the State Committee on Securities supervises the securities sector. The competent authorities appear knowledgeable, well-resourced, and well-trained in AML/CTF issues and conduct inspections regularly. However, only the NBA includes an AML/CTF component in its inspections.

Customer due diligence (CDD) measures derive from a number of laws and regulations. GOA-issued regulations are enforceable, although for the most part a legislative body has not authorized or issued them. The NBA has issued "Methodological Guidance on the Prevention of the Legalization of Illegally Obtained Funds or Other Property Through the Banking System," but this guidance is not law and is not binding. There is no legal provision in the law for sanctioning violations of AML/CTF guidance or regulations. Likewise, there are few customer identification obligations outlined in the law "On Banks." While the law does prohibit the opening of anonymous accounts, it does not require institutions to verify the beneficial owner of an account. Joint stock companies can issue unlimited numbers of bearer shares. There is no particular enhanced due diligence requirement for dealings with PEPs, and Azerbaijani banks lack regulations governing their actions when opening correspondent accounts elsewhere as well as when conducting non face-to-face transactions or establishing relationships in this manner. There are no prohibitions on financial institutions executing transactions with shell banks. Although there is a record-keeping requirement, it lacks clarity regarding the records that need to be retained and provides no possibility for extending the record-keeping time, even when requested by a competent authority. Azerbaijan does not mandate its financial institutions to ensure that their foreign branches and subsidiaries submit to the requirements of the country where their headquarters are located. Bank secrecy provisions do not pose obstacles for law enforcement investigations. A court decision will mandate the lifting of professional secrecy.

Azerbaijan has no law obliging financial institutions to file suspicious transaction reports (STRs) when they suspect or have reasonable grounds to suspect that funds are the proceeds of crime. The NBA issued letters to banks in 2007, generating approximately 500 STRs. Of these, the NBA passed 24 to law enforcement. There is also no legal obligation on financial institutions to report suspicion of terrorist financing to a financial intelligence unit (FIU). Azerbaijani authorities have not conducted any training our outreach with regard to money laundering and terrorist financing. Even the formal financial sector lacks awareness and understanding of AML/CTF issues: one major commercial bank was unaware of STRs and STR reporting. There are no legal obligations for financial institutions to establish AML/CTF programs or designate a compliance officer.

Because there is no effective law, the designated nonfinancial businesses and professions (DNFBPs) have no AML/CTF obligations. There are no competent authorities to serve as the AML/CTF supervisors. Tax advisors, the 800 lawyers, the 94 auditors and accountants (of which none are independent) do not fall under the AML/CTF rubric at all, as authorities consider them to be a small portion of the nonbank sector and low risk. The 150 notaries in Azerbaijan and approximately 1000 dealers in precious metals and stones may have reporting obligations in the future. The Assay Chamber supervises the dealers in previous metals and stones, but lacks any AML/CTF component. Azerbaijan has prohibited gaming and casino activities, although it does run a state lottery.

The MER reported that there appeared to be little coordination at the policy and at the working level between the agencies charged with combating AML/CTF and between the supervisory bodies.

Azerbaijan lacks an FIU. The GOAJ has advised that until adoption of the AML/CTF law, it will not be able to establish an FIU. Currently, the 3-member AML Division of the National Bank of

Azerbaijan (NBA) has taken on some of the functions that an FIU would manage. However, the General Prosecutor's office was unaware of the existence of any suspicious transaction reports (STRs).

Investigatory authority in AML/CTF cases lies ultimately with the General Prosecutor. The Ministry of National Security has also worked with AML/CTF issues, reporting that the majority of STRs relate to terrorist financing. However, few terrorist-related investigations or prosecutions appear to have taken place. Although there are ways that the current criminal law could be effective, the Prosecutor's Office does not use it. Law enforcement authorities have not received training or outreach with regard to money laundering and terrorist financing issues, and lack overall awareness of the offense. They also lack training in financial investigation techniques. While law enforcement overall appears to have proper authority and enough resources, the amount of resources directed to pursuing money launderers as opposed to other crime seems scant. There is an overall perception that prosecutions for money laundering would be very difficult and would not add value to the conviction for the predicate offense. Authorities interpret the money laundering offense to mean self-laundering only and have not considered third party laundering or the use of money laundering in organized crime.

Azerbaijani authorities did not provide statistics regarding asset seizure and confiscation, but told the MONEYVAL assessors that they have issued such orders. The only crimes whose proceeds would be subject to confiscation are money laundering and crimes punishable by two years or more in prison. Because there is no criminal liability for legal persons, the authorities cannot confiscate property from legal persons.

Although the GOAJ has criminalized the financing of terrorism, it has applied a very narrow definition. As the definition now stands, it is not wholly a predicate offense for money laundering. Authorities would also need to provide evidence of financial or material support for specific terrorist acts, as Azerbaijan has not explicitly criminalized the financing of terrorist organizations or an individual terrorist; it also has omitted as a criminal offence the support of recruitment and other activities by terrorist organizations and support of the families of terrorists. Prosecutors have obtained one successful prosecution against an individual collecting money to finance future terrorist acts.

Azerbaijan appears to have instituted a system to implement UNSCR 1267 and 1373, and the Ministry of Foreign Affairs has sent out the lists to other Ministries and supervisory bodies. However, there has been no guidance issued, even to the financial sector, and no one outside the banking sector appears to be aware of the lists. The nonbank sectors have never frozen assets in conjunction with the UNSCRs. There does not appear to be an authority charged with designating persons or entities subject to freezing orders. Since 2003, Azerbaijani authorities have not issued any freezing orders.

Azerbaijan has entered into a number of mutual legal assistance treaties, although the absence of criminal liability for legal or corporate persons and the dual criminality requirement could pose challenges to legal cooperation. Azerbaijan does not have a mutual legal assistance treaty with the United States. Azerbaijan's law enforcement authorities are developing a network of cooperation and information exchange at the intelligence level. Although the lack of an FIU means that Azerbaijan's cooperation with the FIU community is severely hampered, the NBA has responded to requests from two FIUs.

Azerbaijan has ratified the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the UN Convention for the Suppression of the Financing of Terrorism. It is a member of the MONEYVAL Committee.

It is encouraging that the Government of Azerbaijan (GOAJ) will have passed AML/CTF legislation in early 2009 that will provide for the development of a financial intelligence unit. However, that legislation will require amending to conform to international standards. The GOAJ should begin implementing the new legislation through promulgating binding and enforceable regulations for both the financial sectors and the DNFBPs. It should conduct awareness and outreach campaigns for the

entities that will be subject to the law, and work to establish an FIU so that upon passage of the legislation, the FIU will be able to begin its work. Azerbaijan should prohibit bearer shares. The GOAJ should ensure that the regulatory authorities and enforcement agencies have resources targeted specifically to the pursuit of money laundering and terrorist financing/ The GOAJ should provide training, in particular for law enforcement and prosecutors, to enable authorities to conduct complex investigations and obtain convictions. The GOAJ should establish venues for both strategy formulation and coordination and cooperation between the relevant authorities charged with AML/CTF work. The GOAJ should conduct outreach regarding the UN Security Council Resolutions and freezing orders.

Bahamas

The Commonwealth of The Bahamas is an important regional and offshore financial center. The financial services sector provides a vital economic contribution to The Bahamas, accounting for approximately 15 percent of the country's gross domestic product. The U.S. dollar circulates freely in The Bahamas, and is accepted everywhere on par with the Bahamian dollar. Money laundering in The Bahamas is primarily related to financial fraud and the proceeds of drug trafficking. Illicit proceeds from drug trafficking usually take the form of cash or are quickly converted into cash. The strengthening of anti-money laundering laws has made it increasingly difficult for most drug traffickers to deposit large sums of cash. As a result, drug traffickers store extremely large quantities of cash in security vaults at properties deemed to be safe houses. Other money laundering trends include the purchase of real estate, large vehicles and jewelry, as well as the processing of money through a complex web of legitimate businesses, and international business companies registered in the offshore financial sector.

There are presently four casinos operating in The Bahamas, with three new casinos scheduled to open within the next few years. Cruise ships that overnight in Nassau may operate casinos. Reportedly, there are over ten Internet gaming sites based in The Bahamas, although Internet gambling is illegal in The Bahamas. Under Bahamian law, Bahamian residents are prohibited from gambling. The Gaming Board of The Bahamas issues licenses and has anti-money laundering oversight for the gaming industry. Freeport is the only free trade zone in The Bahamas. There are no indications that it is used to launder money.

The financial sector of The Bahamas is comprised of onshore and offshore financial institutions, which include banks and trust companies, insurance companies, securities firms and investment funds administrators, financial and corporate service providers, cooperatives, and societies. Regulated designated nonfinancial businesses and professions include casinos; lawyers; accountants; real estate agents; and company service providers. Dealers in precious metals and stones are not included.

The Bahamas has six financial sector regulators: the Central Bank of the Bahamas, which is responsible for licensing and supervision of banks and trust companies; the Securities Commission, responsible for regulating the securities and investment funds industry; the Compliance Commission, which supervises financial sector businesses that are not subject to prudential supervision such as lawyers and accountants; the Inspector of Financial and Corporate Service Providers (IFCSP), which licenses and supervises company incorporation agents and other financial service providers; the Director of Societies, which regulates credit unions and societies; and the Registrar of Insurance Companies. These six regulators comprise the Group of Financial Sector Regulators (GFSR). The GFSR meets on a monthly basis to facilitate information sharing between domestic and foreign regulators and discuss cross-cutting regulatory issues, including anti-money laundering.

The Central Bank Act 2000 (CBA) and The Banks and Trust Companies Regulatory Act 2000 (BTCRA) enhance the supervisory powers of the Central Bank to conduct on-site and off-site inspections of banks and enhance cooperation between overseas regulatory authorities and the Central

Bank. The BTCRA expands the licensing criteria for banks and trust companies, augments the supervisory powers of the Inspector of Banks and Trust Companies, and enhances the role of the Central Bank Governor. These expanded rights include the right to deny licenses to banks or trust companies deemed unfit to transact business in The Bahamas. In May 2008, amendments to the Banks and Trust Companies Regulation (Amendment) Act 2008 and the Central Bank of Bahamas Act 2008 formally place money transmission businesses under the supervision of the Central Bank. The Banks and Trust Companies (Money Transmission Business) Regulations 2008 requires money transmission agents to register with the Central Bank.

In 2001, the Central Bank enacted a physical presence requirement that means "managed banks" (those without a physical presence but which are represented by a registered agent such as a lawyer or another bank) must either establish a physical presence in The Bahamas (an office, separate communications links, and a resident director) or cease operations. The transition from to full physical presence is complete. Some industry sources have suggested that this requirement has contributed to a decline in shell banks and trusts from 301 in 2003 to 136 as of June 30, 2008.

The International Business Companies Act 2000 and 2001 (Amendments) enacts provisions that abolish bearer shares, require international business companies (IBCs) to maintain a registered office in The Bahamas, and require the registered office to maintain a copy of the names and addresses of the directors and officers and a copy of the shareholders register. A copy of the register of directors and officers must also be filed with the Registrar General. There are approximately 115,000 registered IBCs, only 42,000 of which are active. Only banks and trust companies licensed under the BTCRA and financial and corporate service providers licensed under the Financial Corporate Service Providers Act (FCSPA) may provide registration, management, administration, registered agents, registered offices, nominee shareholders, and officers and directors for IBCs.

The Proceeds of Crime Act 2000 criminalizes money laundering. The POCA provides for four main money laundering offenses: the transfer or conversion of property with the intent to conceal or disguise the property; assisting another to conceal the proceeds of criminal conduct; the acquisition, possession or use of the proceeds of crime; and a legal obligation to make a report to the financial intelligence unit (FIU) or police when it is known or suspected that another person is engaged in money laundering. Individuals found guilty of money laundering can be fined up to $100,000 or imprisoned for up to five years or both, or up to twenty years and/or an unlimited fine. Individuals found guilty of failing to disclose and/or tipping off can be fined up to $50,000 or imprisoned up to three years or up to ten years and/or an unlimited fine.

The Financial Transaction Reporting Act 2000 (FTRA) establishes customer due diligence "know your customer" (KYC) requirements. The FTRA requires the verification of identity of any customer before establishing a business relationship; transactions exceeding $15,000; structured transactions in the amount exceeding $15,000; when it is known or suspected a customer's transaction is the proceeds of crime; doubt of customer's identity; and transactions conducted on behalf of a third party. By December 31, 2001, financial institutions were obliged to verify the identities of all their existing account holders and of customers without an account who conduct transactions over $10,000. All new accounts established in 2001 or later have to be in compliance with KYC rules before they are opened. As of October 2006, the Central Bank reported full compliance with KYC requirements. All nonverified accounts were frozen.

The FTRA is limited to transactions involving cash and does not cover all occasional transactions. Financial institutions are not required to undertake customer due diligence measures when carrying out occasional transactions that are wire transfers. Enforceable requirements related to politically exposed persons (PEPs) are applicable only to banks and trust companies through the Central Bank's AML/CTF Guidelines. Non-enforceable provisions regarding PEPs were adopted by the Securities Commission's Guidelines and the Compliance Commission's Code of Practice. In December 2008,

amendments were passed to the FTRA, the Securities Industry Act, the Financial Service and Corporate Providers Act, and the Financial Intelligence Unit Act to address these deficiencies and bring The Bahamas into compliance with international standards for customer due diligence. The amendments provide for the enforceability of the guidelines, codes, procedures, and rules issued by regulators other than the Central Bank.

The Bahamas financial intelligence unit (FIU), established by the FIU Act 2000, operates as an independent administrative body under the Office of the Attorney General, and is responsible for receiving, analyzing and disseminating suspicious transaction reports (STRs). The FTRA requires financial and nonfinancial institutions to report suspicious transactions to the FIU when the institution suspects or has reason to believe that any transaction involves the proceeds of crime. The FIU Act 2000 protects obligated entities from criminal or civil liability for reporting transactions. Financial institutions are required by law to maintain records related to financial transactions for no less than five years. The FIU has the administrative power to issue an injunction to stop anyone from completing a transaction for a period of up to three days upon receipt of an STR. The FIU receives approximately 100-150 STRs annually; most are related to suspicions of fraud, corruption and drug trafficking. If money laundering or terrorist financing is suspected, the FIU will disseminate STRs to the Tracing and Forfeiture/Money Laundering Investigation Section (T&F/MLIS) of the Drug Enforcement Unit (DEU) of the Royal Bahamas Police Force for investigation and prosecution in collaboration with the Office of the Attorney General. Data on STRs received in 2008 was unavailable prior to the annual report published by FIU in early 2009.

The FIU is responsible for publishing guidelines to advise entities of their reporting obligations. In March 2007, the FIU revised its guidelines to incorporate terrorist financing reporting requirements. These new guidelines give financial institutions information on requirements that must be met, how to identify suspicious transactions, and how to report these transactions to the FIU. The FIU plans to implement the National Strategy to Prevent Money Laundering in early 2009. The strategy arose in response to recommendations from the Financial Action Task Force (FATF) and will provide a means to ensure compliance with international anti-money laundering standards.

As a matter of law, the Government of the Commonwealth of the Bahamas (GOB) seizes assets derived from international drug trade and money laundering. The banking community has cooperated with these efforts. During 2008, nearly $4 million in cash and assets were seized or frozen. The seized items are in the custody of the GOB. Some are in the process of confiscation while some remain uncontested. Seized assets may be shared with other jurisdictions on a case-by-case basis.

In 2004, the Anti-Terrorism Act (ATA) was enacted to implement the provisions of the UN International Convention for the Suppression of the Financing of Terrorism and UN Security Council Resolution 1373 and make provision for preventing and combating terrorism. In addition to formally criminalizing terrorism and making it a predicate crime for money laundering, the law provides for the seizure and confiscation of terrorist assets, reporting of suspicious transactions related to terrorist financing, and strengthening of existing mechanisms for international cooperation. The ATA was amended in 2008 to clarify aspects of the legislation and further comply with UN Conventions related to terrorist financing. In 2007, The Royal Bahamas Police Force established a Special Anti-Terrorism Unit to investigate cases of terrorism and terrorist financing.

The Royal Bahamas Police Force (RBPF) has cooperated with the U.S. Immigration and Customs Enforcement (ICE) in various financial investigations, including sharing of records and other financial data. In 2008, ICE obtained the cooperation of RBPF officials with the identification of subjects and assets identified as relating to or generated by money laundering activities, particularly pertaining to the smuggling of bulk currency, a preferred method for drug dealers and other criminals to move illicit proceeds across international borders. Between January 2000 and September 2008, 17 individuals were charged with money laundering by the Royal Bahamas Police Force's T&F/MLIS, leading to

seven convictions. Seven defendants await trial, while two defendants fled the jurisdiction prior to trial.

The Bahamas is a member of the Offshore Group of Banking Supervisors and the Caribbean Financial Action Task Force (CFATF), a FATF-style regional body. The FIU has been an active participant within the Egmont Group since becoming a member in 2001, and is currently one of the two regional representatives for the Americas. The Bahamas FIU has the ability to sign memoranda of understanding (MOUs) with other counterpart FIUs to exchange information.

The Bahamas is a party to the UN 1988 Drug Convention, and the UN International Convention for the Suppression of the Financing of Terrorism. In 2008, The Bahamas became a party to both the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. The Bahamas has an information exchange agreement with the U.S. Securities and Exchange Commission to ensure that requests can be completed in an efficient and timely manner. The Bahamas has a Mutual Legal Assistance Treaty (MLAT) with the United States, which entered into force in 1990, and agreements with the United Kingdom and Canada. Recently, several successful cases involving asset sharing have occurred between the United States and the Bahamas resulting in large amounts being shared by each government with the other.

The Government of the Commonwealth of The Bahamas should continue to enhance its anti-money laundering and counterterrorist financing regime by implementing the National Strategy on the Prevention of Money Laundering. It should also ensure that there is a public registry of the beneficial owners of all entities licensed in its offshore financial center. The Bahamas should also provide adequate resources to its law enforcement, prosecutorial and judicial entities to ensure that investigations and prosecutions are satisfactorily completed and requests for international cooperation are efficiently processed.

Bahrain

Bahrain is an important international financial center in the Gulf region. In contrast with its Gulf Cooperation Council (GCC) neighbors, Bahrain has a service based economy, with the financial sector providing more than 20 percent of GDP. It hosts a diverse group of financial institutions, including 195 banks, of which 57 are wholesale banks (formerly referred to as off-shore banks or OBUs); 46 investment banks; and 26 commercial banks, of which 19 are foreign-owned. There are 35 representative offices of international banks. Bahrain has 38 Islamic banks and financial institutions. There are 22 moneychangers and money brokers, and several other investment institutions, including 87 insurance companies. While Bahrain is not a major money laundering country, the greatest risk of money laundering stems from foreign proceeds that transit through the country. The vast network of Bahrain's banking system, along with its geographical location in the Middle East as a transit point along the Gulf and into Southwest Asia, may attract money laundering activities.

In January 2001, the Government of Bahrain (GOB) enacted an anti-money laundering law (AML) that criminalizes the laundering of proceeds derived from any predicate offense. The law stipulates punishment of up to seven years in prison, and a fine of up to one million Bahraini dinars (approximately $2.66 million) for convicted launderers and those aiding or abetting them. If organized criminal affiliation, corruption, or a disguised origin of proceeds is involved, the minimum penalty is a fine of at least 100,000 dinars (approximately $266,000) and a prison term of not less than five years.

The 2001 AML was amended in August 2006 by Law 54/2006, which criminalizes the undeclared transfer of money across international borders for the purpose of money laundering or in support of terrorism. Anyone convicted under the law of collecting or contributing funds, or otherwise providing financial support to a group or persons who practice terrorist acts, whether inside or outside Bahrain, will be subject to imprisonment for a minimum of ten years in prison up to a maximum of a life

sentence. The law also stipulates a fine of between the equivalent of $26,700 and $1.34 million. Law 54 also codified a legal basis for a disclosure system for cash couriers, though supporting regulations must still be enacted. In June 2008, the government moved to increase supervision of its borders, by placing Ports and Customs inspections under the Ministry of Interior. The Ministry of Interior subsequently instructed its officials to strictly enforce laws against the illegitimate movement of currency.

A controversial provision of Law 54 is a revised definition of terrorism that is based on the Organization of the Islamic Conference definition. Article 2 excludes from the definition of terrorism acts of struggle against invasion or foreign aggression, colonization, or foreign supremacy in the interest of freedom and the nation's liberty.

Under the 2001 AML law, the Bahrain Monetary Agency (BMA) was the principal financial sector regulator and de-facto central bank, issuing regulations and requiring financial institutions to file suspicious transaction reports (STRs), to maintain records for a period of five years, and to provide ready access for law enforcement officials to account information. Immunity from criminal or civil action is given to those who report suspicious transactions. Even prior to the enactment of Law 54, financial institutions were obligated to report suspicious transactions greater than 6,000 dinars (approximately $16,000) to the BMA/Central Bank. The current requirement for filing STRs stipulates no minimum thresholds and since 2005 the BMA/Central Bank has had a secure online website that banks and other financial institutions can use to file STRs.

In September 2006, Law 64/2006 replaced the BMA with the Central Bank of Bahrain (CBB). Law 64 consolidated several laws that had previously governed the various segments of the financial services industry. Under the law, the CBB enjoys reinforced operational independence and enhanced enforcement powers. Part 9 of the law, for example, outlines investigational and administrative proceedings at the CBB's disposal to ensure licensee compliance with rules and regulations. The CBB's compliance arm was upgraded from a unit to a directorate.

The 2001 AML law also provided for the formation of an interagency committee to oversee Bahrain's anti-money laundering regime. Accordingly, in June 2001, the Policy Committee for the Prohibition and Combating of Money Laundering and Terrorist Financing was established and assigned the responsibility for developing anti-money laundering policies and guidelines. In early 2006, the chairmanship of the Policy Committee was transferred from the Ministry of Finance to the CBB. The Committee's membership was also expanded, to comprise representatives from the Ministries of Finance, Industry and Commerce, Interior, and Social Development; the Directorates of Customs and Legal Affairs; the Office of Public Prosecution; the National Security Agency; the Bahrain Stock Exchange; and the CBB.

In addition, the 2001 AML law provided for the creation of the Anti-Money Laundering Unit (AMLU) as Bahrain's financial intelligence unit (FIU). The AMLU, which is housed in the Ministry of Interior, is empowered to receive suspicious transaction reports (STRs); conduct investigations; implement procedures relating to international cooperation under the provisions of the law; and execute decisions, orders, and decrees issued by the competent courts in offenses related to money laundering. The AMLU became a member of the Egmont Group of FIUs in July 2003.

The AMLU receives STRs from banks and other financial institutions, investment houses, broker/dealers, moneychangers, insurance firms, real estate agents, gold dealers, financial intermediaries, and attorneys. Financial institutions must also file STRs with the Central Bank, which supervises these institutions. Nonfinancial institutions are required under a Ministry of Industry and Commerce (MOIC) directive to also file STRs with that ministry. The Central Bank analyzes the STRs, of which it receives copies, as part of its scrutiny of compliance by financial institutions with anti-money laundering and counterterrorist financing (AML/CTF) regulations, but it does not

independently investigate the STRs as the responsibility for investigation rests with the AMLU. The Central Bank may assist the AMLU with its investigations where special banking expertise is required.

The Central Bank of Bahrain is the regulator for other nonbanking financial institutions including insurance companies, exchange houses, and capital markets. The Central Bank inspected eight insurance companies in 2007 and had conducted eleven more inspections by October 2008. Additional insurance industry inspections are scheduled for 2009. Anti-money laundering regulations for investment firms and securities brokers were revised in April 2006.

In November 2007, the MOIC published new anti-money laundering guidelines, which govern designated nonfinancial businesses and professions (DNFBPs). The MOIC has announced an increased focus on enforcement, including car dealers, jewelers, and real estate agencies noting 274 visits to DNFBPs in 2007, and 271 through October 2008. Of the 271 visits in 2008, 145 were assigned an MOIC compliance officer as a result. The MOIC has also increased its inspection team staff from seven to nine.

The MOIC system of requiring dual STR reporting to both it and the AMLU mirrors the Central Bank's system. Good cooperation exists between MOIC, Central Bank, and AMLU, with all three agencies describing the double filing of STRs as a backup system. The AMLU and Central Bank's compliance staff analyze the STRs and work together on identifying weaknesses or criminal activity, but it is the AMLU that must conduct the actual investigation and forward cases of money laundering and terrorist financing to the Office of the Public Prosecutor.

From January through December 2008, the AMLU has received and investigated 201 STRs, 42 of which have been forwarded to the courts for prosecution. The GOB completed its first successful money laundering prosecution in May 2006. The prosecutions resulted in the convictions of two expatriate felons with sentences of one and three years and fines of $380 and $1900 respectively.

In October 2007 the government used the new AML/CTF law of 2006 to bring charges against five suspects. In January 2008, they were convicted of a range of charges, including the financing of terrorism. The five were sentenced to six months' imprisonment. In June 2008, authorities arrested two Bahrainis on charges of financing terrorism. The case remained pending as of December 2008.

Bahrain is moving ahead with plans to establish a special court to try financial crimes, and judges are undergoing special training to handle such crimes. Six Bahraini judges will join a group of twelve Jordanian judges on loan to the Ministry of Justice to serve on the court, which is expected to begin hearing cases in September 2009.

There are 57 Central Bank-licensed wholesale banks (formerly referred to as offshore banking units OBUs) that are branches of international commercial banks. The license that changed OBUs to wholesale banks allows wholesale banks to accept deposits from citizens and residents of Bahrain, and undertake transactions in Bahraini dinars (with certain exemptions, such as dealings with other banks and government agencies). In all other respects, wholesale banks are regulated and supervised in the same way as the domestic banking sector. They are subject to the same regulations, on-site examination procedures, and external audit and regulatory reporting obligations.

However, Bahrain's Commercial Companies Law (Legislative Decree 21 of 2001) does not permit the registration of offshore companies or international business companies (IBCs). All companies must be resident and maintain their headquarters and operations in Bahrain. Capital requirements vary, depending on the legal form of company, but in all cases the amount of capital required must be sufficient for the nature of the activity to be undertaken. In the case of financial services companies licensed by the Central Bank, various minimum and risk-based capital requirements are also applied in line with international standards of Basel Committee's "Core Principles for Effective Banking Supervision."

BMA Circular BC/1/2002 states that money changers may not transfer funds for customers in another country by any means other than Bahrain's banking system. In addition, all Central Bank licensees are required to include details of the originator's information with all outbound transfers. With respect to incoming transfers, licensees are required to maintain records of all originator information and to carefully scrutinize inward transfers that do not contain the originator's information, as they are presumed to be suspicious transactions. Licensees that suspect, or have reasonable grounds to suspect, that funds are linked or related to suspicious activities-including terrorist financing-are required to file STRs. Licensees must maintain records of the identity of their customers in accordance with the Central Bank's anti-money laundering regulations, as well as the exact amount of transfers. During 2004, the BMA consulted with the industry on changes to its existing AML/CTF regulations, to reflect revisions by the FATF to its Forty plus Nine Recommendations. Revised and updated BMA regulations were issued in mid-2005.

Legislative Decree No. 21 of 1989 governs the licensing of nonprofit organizations. The Ministry of Social Development (MSD) is responsible for licensing and supervising charitable organizations in Bahrain. In February 2004, as part of its efforts to strengthen the regulatory environment and fight potential terrorist financing, MSD issued a Ministerial Order regulating the collection of donated funds through charities and their eventual distribution, to help confirm the charities' humanitarian objectives. The regulations are aimed at tracking money that is entering and leaving the country. These regulations require organizations to keep records of sources and uses of financial resources, organizational structure, and membership. Charitable societies are also required to deposit their funds with banks located in Bahrain and may have only one account in one bank. Banks must report to the Central Bank any transaction by a charitable institution that exceeds 3,000 Bahraini dinars (approximately $8,000). MSD has the right to inspect records of the societies to insure their compliance with the law. The Directorate of Development and Local Societies (DDLS) has a very small staff to undertake the necessary reviews of the financial information submitted by societies or to undertake inspections of these organizations

Bahrain is a leading Islamic finance center in the region. The sector has grown considerably since the licensing of the first Islamic bank in 1979. Bahrain has 38 Islamic banks and financial institutions. Given the large share of such institutions in Bahrain's banking community, the Central Bank has developed an appropriate framework for regulating and supervising the Islamic banking sector, applying regulations and supervision as it does with respect to conventional banks. In March 2002, the Central Bank introduced a comprehensive set of regulations for Islamic banks called the Prudential Information and Regulatory Framework for Islamic Banks (PIRI). The framework was designed to monitor certain banking aspects, such as capital requirements, governance, control systems, and regulatory reporting.

Bahrain does not have a mutual legal assistance agreement with the United States. Bahrain is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention for the Suppression of the Financing of Terrorism. Bahrain is not a party to the UN Convention against Corruption. In January 2002, the BMA issued a circular implementing the Financial Action Task Force (FATF) Special Recommendations on Terrorist Financing as part of the Central Bank's AML regulations. Bahrain hosts the Secretariat and is a member of the Middle East and North Africa Financial Action Task Force (MENFATF), a FATF-style regional body that was established 2004. In November 2006, MENAFATF approved the mutual evaluation report on Bahrain.

The Government of Bahrain has demonstrated a commitment to establish a strong anti-money laundering and terrorist financing system and appears determined to engage its large financial sector in this effort. The AMLU should maintain its efforts to obtain and solidify the necessary expertise in tracking suspicious transactions. Nevertheless, there should not be an over-reliance on suspicious transaction reporting to initiate money laundering investigations. Authorities should continue to raise awareness within the capital markets and designated nonfinancial businesses and professions

regarding STR reporting obligations and consider applying sanctions for willful noncompliance. Adequate resources should be devoted to the Ministry of Social Development to increase its oversight of NGOs and charities. Supporting regulations should be enacted and enforced governing bulk cash smuggling. Bahrain should become a party to the UN Convention against Corruption.

Bangladesh

Bangladesh is not a regional or offshore financial center. Under the caretaker government that declared a state of emergency when it came to power on January 11, 2007, evidence of funds laundered through the official banking system escalated. The new government instituted a stringent anticorruption campaign that netted more than $180 million in proceeds—a fraction of the estimated total amount of corrupt funds located both domestically and abroad. Fighting corruption is a keystone of the caretaker government under the state of emergency. Money transfers outside the formal banking and foreign exchange licensing system are illegal and therefore not regulated. The principal money laundering vulnerability remains the widespread use of the underground hawala or "hundi" system to transfer money and value outside the formal banking network. The vast majority of hundi transactions in Bangladesh are used to repatriate wages from expatriate Bangladeshi workers.

The Central Bank (CB) reports a considerable increase in remittances since 2002 through official channels. The figure more than doubled from $2 billion to $4.3 billion in fiscal year 2006 (July 1-June 30) and then rose again to $5.9 billion in fiscal year 2007 and $7.9 billion in fiscal year 2008. The increase is due to competition from commercial banks through improved delivery time, guarantees, and value-added services such as group life insurance. However, hundi remains entrenched because it is used to avoid taxes, customs duties, and currency controls. The nonconvertibility of the local currency (the taka) coupled with intense scrutiny on foreign currency transactions in formal financial institutions also contribute to the popularity of hundi and black market money exchanges.

In Bangladesh, hundi primarily uses trade goods to provide counter valuation or a method of balancing the books in transactions. It is part of trade-based money laundering and a compensation mechanism for the significant amount of goods smuggled into Bangladesh. An estimated $1 billion dollars worth of dutiable goods are smuggled every year from India into Bangladesh. A comparatively small amount of goods are smuggled out of the country into India. Hard currency and other assets flow out of Bangladesh to support the smuggling networks.

The Government of Bangladesh (GOB) realized that it did not have a mechanism to request assistance from other nations to help track illegal proceeds flowing overseas, some of which is related to corruption and capital flight. As a result, in February 2007 the GOB acceded to the UN Convention against Corruption (UNCAC). Pursuant to UNCAC, the GOB designated the Attorney General's Office as the central authority for mutual legal assistance requests. In August 2008, Bangladesh signed the South Asian Association for Regional Cooperation (SAARC) Convention on Mutual Assistance in Criminal Matters. Using UNCAC as the legal basis, the government has so far sent Mutual Legal Assistance Requests on tracing, freezing and seizure to foreign jurisdictions.

In April and June 2008 the government promulgated the Money Laundering Prevention Ordinance (MLPO 2008) and the Anti-Terrorism Ordinance (ATO 2008). The laws facilitate international cooperation in recovering money illegally transferred to foreign countries and mutual legal assistance in terms of criminal investigation, trial proceedings, and extradition matters. The GOB has formed a national level committee headed by the Law Adviser and an inter-agency Task Force headed by the Governor of the CB to retrieve illegally transferred money.

For the past twenty years, corrupt practices became so common that, between 2001 and 2005, Transparency International ranked Bangladesh in its Corruption Perception Index as the country with the highest level of perceived corruption in the world. In 2008, Bangladesh was ranked 147 out of 180

countries surveyed. Bangladeshis are not allowed to carry cash outside of the country in excess of the equivalent of $3,000 to South Asian Association for Regional Cooperation (SAARC) countries and the equivalent of $5,000 to other countries. Proper documents are required by authorized foreign exchange banks and dealers. The GOB does not place a limit on how much currency can be brought into the country, but amounts over $5,000 must be declared within 30 days. The Customs Bureau is primarily a revenue collection agency, accounting for 40-50 percent of Bangladesh's annual government income.

The MLPO of 2008 introduced a new set of financial organizations that must report to the CB regarding their activities in a manner similar to that of banks and financial institutions. These reporting organizations (ROs) include insurance companies, money changers and remitters, fund-transfer companies or organizations, and companies permitted to operate as business organizations under the CB's authority. The CB also has the right to notify other organizations that they must function as ROs for purposes of the MLPO of 2008. The inclusion of these new ROs pose new regulatory and oversight challenges for the CB's Anti-Money Laundering Department (AMLD) In addition, the GOB regulates insurance companies and money changers and remitters under the Foreign Exchange Regulation Act (FERA), 1947.

The CB regularly conducts training, conferences and seminars for the staff and officers of 48 commercial banks around the country regarding "know your customer" procedures. The CB carries out additional training focusing on identifying suspicious and cash transactions and reporting them to the CB, where the country's financial intelligence unit (FIU) is located.

In May 2007, the GOB identified the CB's AMLD as Bangladesh's financial intelligence unit (FIU). The MPLO of 2008 officially established the existence of the FIU. The FIU depends on the CB for its operation and budget. The CB enjoys complete operational and budgetary independence. An Executive Director of the CB heads the FIU, which consists of approximately 25 officials.

The MLPO of 2008 allows the FIU to enter into agreements and arrangements with foreign FIUs to receive and request information in relation to money laundering offenses or suspicious transactions. In August 2008, the FIU signed its first Memorandum of Understanding (MOU) with the Malaysia's FIU to facilitate the exchange of information on money laundering, terrorism financing, and related criminal activity. In October 2008, the FIU signed its second MOU with the Nepal's FIU. The FIU is negotiating similar agreements with other counterparts. However, many counterparts require that the Bangladesh FIU be a member of the international association of FIUs, the EGMONT Group, before negotiating MOUs with Bangladesh.

The recently enacted ordinances, MLPO 2008 and ATO 2008, enhance the powers and responsibilities of the CB and its FIU in many ways. The CB is empowered and authorized to analyze suspicious transaction reports (STRs) and cash transaction reports (CTRs) and maintain a financial intelligence database and related information. In September 2007, the Cash Transaction Report (CTR) threshold increased from 500,000 to 700,000 takas (approximately $10,250). The CB may call for and receive from ROs any information related to transactions where there are reasonable grounds to suspect the transaction involves money laundering and/or terrorist financing. The CB can direct ROs to take measure to combat money laundering and terrorist financing activities. Overall, the CB can monitor and observe the activities of banks as well as nonbanking institutions. The CB can, if necessary, conduct on-site inspection of ROs. Finally, the CB can arrange training, conferences and seminars for all ROs. The FIU spearheads national efforts and promotes national awareness in detecting and preventing money laundering and terrorism financing.

The new ordinances allows the CB, without a court order, to order any bank or financial institution to suspend a transaction or freeze an account for a period of 30 days when there are reasonable grounds to suspect that a transaction involves the proceeds of a crime. The CB may extend such orders for an additional 30 days for the purpose of further investigation. The CB is authorized to have access to the

information of bank accounts of any individual or company on demand without a court order if the CB has reasonable grounds to suspect that a transaction involves the proceeds of a crime.

The MLPO of 2008 designates the Anti-Corruption Commission (ACC), established pursuant to the Anti-Corruption Commission Act, 2004, as the national Investigating Organization (IO) regarding money laundering matters. Any official empowered to act on behalf of ACC may be considered part of the IO. The Bangladesh police are in charge of investigating crimes under ATO 2008. Under separate authorities, the National Board of Revenue (NBR), the country's tax authority, is allowed to freeze an account without a court order for tax purposes only. Under the MLPO of 2008, on an application of the IO, a court may pass a freezing or attachment order on the property of the accused, situated within or outside Bangladesh, in which the people of the state have interest. The law allows for only conviction based forfeiture against the property connected to the crime.

The ACC is not adequately staffed and trained to handle money laundering investigations. Media accounts and discussions with ACC staff indicate that the ACC has largely confined itself to gathering records of the assets of corruption suspects and using them to pursue less complicated criminal cases. The offense of "Amassing wealth through illegal means beyond known source of income" is a typical charge brought against suspects investigated by the ACC. The MLPO of 2008 requires the ACC prove one of the designated predicate offenses in order to successfully prosecute the crime of money laundering. The MLPO of 2008 lists 16 predicate offenses, including corruption and bribery; counterfeiting currency or documents; extortion; fraud; forgery; and illicit trafficking in persons or arms or narcotic drugs and psychotropic substances. Under the prior money laundering law (MLPA 2002), the ACC was not required to prove a predicate offense. The money laundering prosecutions currently pending have been carried out pursuant to MLPA 2002.

Following passage of MLPA 2002, the GOB made the now defunct Bureau of Anti-Corruption (BAC) responsible for taking legal steps regarding money laundering crimes. Between 2002 and 2004, BAC filed 35 cases for money laundering. The ACC had no jurisdiction to initiate legal steps on money laundering charges until the middle of 2007, when the offence was included in the ACC Act 2004.

In recent years, Bangladesh law enforcement has made little progress in pursuing money laundering investigations, in part due to difficulties in procedure and inter-agency cooperation. A major setback occurred in December 2005 when the newly created ACC advised the CB that it would not investigate money laundering cases and returned them to the CB. As a result, the Criminal Investigation Division of the national police force agreed to investigate the cases. During 2006, the CB and police hammered out a procedure to pursue investigations initiated through suspicious transactions reports. The State of Emergency in 2007 brought a differently-configured law enforcement regime headed by military officers. The government set up ten fast-track courts to try graft suspects. As of October 2008, the ACC and the NBR had filed 244 cases in the fast-track courts. Of those cases, the court delivered verdicts in 122 cases. Most of the remaining cases were stayed at different stages by the Supreme Court. The court stayed some cases before charge framing, some after charge framing, and others just before the delivery of verdict. When verdicts were delivered, the court passed confiscation and forfeiture orders in most cases. The ACC has so far won two money laundering cases in 2008. Both cases were tried under MLPA 2002. In October 2008, the International Criminal Police Organization (Interpol) detected laundered money deposited with a Hong Kong bank by a former BNP minister and his son. ACC is currently working on the case.

Bangladesh authorities have not yet tried any cases under the newly enacted ATO 2008. According to published media reports, the trials of Jama'atul Mujahideen Bangladesh (JMB) members responsible for staging over 400 bombings around Bangladesh in August 2005 were mostly conducted under the Arms Act 1878 and the Explosive Substances Act 1908. As of August 2008, the Bangladesh courts completed 77 trials, during which 271 JMB leaders and activists were convicted. As a result, the courts have awarded 41 death sentences, 98 terms of life imprisonment and 132 different other jail

terms. Intelligence officials told news media that 72 persons were acquitted in the cases, as allegations against them were not proved.

The ATO of 2008 authorizes the filing of STRs related to terrorist finance, empowers the CB to monitor suspect financial transactions related to terror finance and prohibits a person from enjoying or possessing property or proceeds of terrorist activity. Property or proceeds of terrorist activity, which is in the possession of a terrorist or a person who is or is not an accused or convicted under the provisions of the ordinance, is liable to be confiscated and forfeited in favor of the government. A judge may pass an order of forfeiture/seizure of proceeds of terrorist activity if he or she is satisfied that such property was seized or confiscated because of its terrorist-related nature.

Since Bangladesh only began in mid-2007 to develop a national identity card (in the form of a voter registration card) and because the vast majority of Bangladeshis do not have a passport, there are difficulties in enforcing customer identification requirements. In most cases, banking records are maintained manually. Some accounting procedures used by the Central Bank do not always achieve international standards. In 2004, the Central Bank issued "Guidance Notes on Prevention of Money Laundering" and designated anti-money laundering compliance programs as a "core risk" subject to the annual bank supervision process of the CB. Banks are required to have an anti-money laundering compliance unit in their head office and a designated anti-money laundering compliance officer in each bank branch. The CB conducts regular training programs for compliance officers based on the Guidance Notes and routinely works with the banks and, if need be, investigates compliance with regulations to curb financial irregularities. Instructors from the CB also conduct regional workshops.

Since the Money Laundering Prevention Act (MLPA) was enacted in 2002, the Central Bank has received approximately 483 STRs. Between April and October 2008, ROs submitted 23 STRs to the CB. Since 2003, Bangladesh has frozen nominal sums in accounts of three designated entities on the UNSCR 1267 Sanctions Committee's consolidated list. In 2004, following investigation of the accounts of an entity listed on the UNSCR 1267 consolidated list, the Central Bank fined two local banks for failure to comply with CB regulatory directives.

In 2005, Bangladesh became a party to the UN International Convention for the Suppression of the Financing of Terrorism. Bangladesh is also a party to the 1988 UN Drug Convention and the UN Convention against Corruption. Bangladesh is not a signatory to the Convention against Transnational Organized Crime.

Bangladesh is a member of the Asia-Pacific Group (APG), a Financial Action Task Force-style regional body. In August 2008, a regional team of experts visited Bangladesh as part of APG's mutual evaluation of the country's safeguards against money laundering and terrorism financing. Earlier in 2008, the GOB formed a National Coordination Committee and a Working Level Committee to prepare for the visit. In the coming year, Bangladesh will face the twin challenges of successfully completing the evaluation and implementing the recommendations of the APG. The GOB has expressed interest in membership in the EGMONT Group, signing MOUs with other FIUs for intelligence gathering and sharing purposes, effectively analyzing and employing STRs/CTRs, and establishing an effective inter-agency working relationship with national stakeholders (law enforcement, regulators and other authorities).

Although positive legislation has been passed and progress has been made, the Government of Bangladesh should continue to strengthen its anti-money laundering/terrorist finance regime so that it adheres to world standards. The GOB should support technology enhancements to reporting channels from outlying districts to the Central Bank. While the FIU is growing steadily, the FIU analysts and investigators need to enhance their ability to conduct analysis, investigations, understand money laundering and terror finance methodologies and guide the ROs. Bangladesh law enforcement and customs should examine forms of trade-based money laundering and initiate money laundering and financial crimes investigations at the "street level" instead of waiting for a STR to be filed with the

FIU. A crackdown on pervasive customs fraud would add new revenue streams for the GOB. Continued efforts should be made to fight corruption, which is intertwined with money laundering, smuggling, customs fraud, and tax evasion. The GOB should ratify the UN Convention against Transnational Organized Crime.

Barbados

Barbados remains vulnerable to money laundering, which primarily occurs in the formal banking system. Domestically, money laundering is largely drug-related and appears to be derived from the trafficking of cocaine and marijuana, as Barbados is a transit country for illicit narcotics. There is also evidence of Barbados being exploited in the layering stage of money laundering with funds originating abroad. The major source of these funds appears to be connected to fraud.

As of October 2008, there are six commercial banks in Barbados. The offshore sector includes 3,334 international business companies (IBCs), compared to 3,615 in 2007,163 exempt insurance companies and 65 qualified exempt insurance companies, five mutual funds companies and one exempt mutual fund company, seven trust companies, five finance companies, and 57 offshore banks. There are no free trade zones and no domestic or offshore casinos.

The International Business Companies Act (1992) provides for the general administration of IBCs. The Ministry of Industry and International Business vets and grants licenses to IBCs after applicants register with the Registrar of Corporate Affairs. The International Business (Miscellaneous Provisions) Act 2001 enhances due diligence requirements for IBC license applications and renewals. Bearer shares are not permitted, and financial statements of IBCs are audited if total assets exceed $500,000.

The Central Bank regulates and supervises domestic and offshore banks, trust companies, and finance companies. The Ministry of Finance issues banking licenses after the Central Bank receives and reviews applications, and recommends applicants for licensing. The International Financial Services Act (IFSA) requires offshore applicants to disclose directors' and shareholders' names and addresses. Offshore banks must submit quarterly statements of assets and liabilities and annual balance sheets to the Central Bank. The Central Bank has the mandate to conduct on-site examinations of offshore banks. This allows the Central Bank to augment its off-site surveillance system of reviewing anti-money laundering (AML) policy documents and analyzing prudential returns. Additionally, permission must be obtained from the Central Bank to move currency abroad.

The Government of Barbados (GOB) criminalizes drug money laundering through the Proceeds of Crime Act and the Drug Abuse (Prevention and Control) Act, 1990-14. The Money Laundering (Prevention and Control) Act 1998 (MLPCA) and subsequent amendments extend the offense of money laundering beyond drug-related crimes by criminalizing the laundering of proceeds from unlawful activities. Under the MLPCA, money laundering is punishable by a maximum of 25 years in prison and a maximum fine of $1,000,000. The MLPCA applies to a wide range of financial institutions, including domestic and offshore banks, IBCs, insurance companies, money remitters, investment services, and any other services of a financial nature. These institutions are required to identify their customers, cooperate with domestic law enforcement investigations, report and maintain records of all transactions exceeding $5,000 for a period of five years, and establish internal audit and compliance procedures. Customer due diligence measures include customer identification and due diligence; beneficial ownership requirements; and, enhanced due diligence for new technologies and correspondent banking, and for high risk customers such as politically exposed persons and non-face-to-face customers. Financial institutions are required to conduct on-going due diligence on business relationships engaging in exchanges of $10,000 or more, and all instructions for international funds transfers of $10,000 or those transiting Barbados. Financial institutions must also report suspicious transactions to the Anti-Money Laundering Authority (AMLA). Tipping off is prohibited.

In 2007, the Central Bank revised the AML guidelines for licensed financial institutions to reflect a risk-based approach, and to include guidance on how licensees can fulfill their obligations in relation to combating terrorist financing. The guidelines apply to all entities that are incorporated in Barbados and are licensed under the Financial Institutions Act 1996 (FIA) and the IFSA. The Central Bank conducts off-site surveillance and undertakes regular on-site examinations of licensees to assess compliance with AML legislation and regulations. Licenses can be revoked by the Minister of Finance for noncompliance. In 2008, the GOB announced its intentions to consolidate regulatory functions into a single agency (except for the Central Bank) to enhance supervision. The proposed Financial Services Commission (FSC) will include: the Office of the Registrar of Co-operatives and Friendly Societies; the Office of Supervisor of Insurance and Pensions; the Securities Commission; and the regulatory and supervisory functions of the office of the Director of International Business. The FSC will regulate nonbanking activities including insurance, pensions, credit unions, securities and mutual funds.

Established by the MLPCA, the AMLA supervises financial institutions' compliance with the MLPCA, and issues training requirements and regulations for financial institutions. The AMLA is comprised of nine members including a chairperson, selected from the private sector; a deputy chairperson, from the University of the West Indies; the Solicitor General; the Commissioner of Police; the Commissioner of Inland Revenue; Comptroller of Customs; the Supervisor of Insurance; the Registrar of Corporate Affairs; and a representative of the Central Bank. The Barbados Financial Intelligence Unit (FIU) is the operational arm of the AMLA and carries out the AMLA's supervisory function over financial institutions.

Established in 2000, the FIU is an independent agency housed in the office of the Attorney General. The FIU is responsible for: receiving and analyzing suspicious activity reports (SARs) from financial institutions; instructing financial institutions to take steps to facilitate an investigation; and, conducting awareness training in regard to record keeping and reporting obligations. There are no laws that prevent disclosure of information to relevant authorities, and persons who report to the FIU are protected under the law.

Financial institutions are required to report transactions when the entity has reasonable grounds to suspect the transaction involves the proceeds of crime or the financing of terrorism, or is suspicious in nature. In cases where the FIU suspects a transaction involves the proceeds of crime, the FIU will forward the report for further investigation to the Commissioner of Police. Between January 1, 2008 and June 30, 2008, the FIU had received 76 SARs; none were referred to the Commissioner of Police. Government entities and financial institutions are required to provide the FIU with information requested by the Director of the FIU. The Royal Barbados Police Force pursues all potential prosecutions.

Barbados has a cross-border reporting system for all persons carrying BDS 10,000 (approximately $5,000) entering and leaving Barbados. Customs has the ability to share information on declarations and seizures with domestic and foreign counterparts. It should be noted that suspicion of money laundering, terrorist financing, or making a false declaration does not provide a basis for stopping and seizure of currency and negotiable instruments. The Money Laundering Financing of Terrorism (Prevention and Control) Act (MLFTA) contains provisions to control bulk cash smuggling and the use of cash couriers.

The MLPCA provides for criminal asset seizure and forfeiture. In 2001, the GOB amended legislation to shift the burden of proof to the accused to demonstrate that property in his or her possession or control is derived from a legitimate source. Absent such proof, the presumption is that such property was derived from the proceeds of crime. The law also enhances the GOB's ability to freeze bank accounts and to prohibit transactions from suspect accounts. Legitimate businesses and other financial institutions are subject to criminal sanction, which can result in the termination of operating licenses. Tracing, seizing and freezing assets may be done by the FIU and the police. Freezing orders are

usually granted for six months at a time after which they need to be reviewed. Frozen assets may be confiscated on application by the Director of Public Prosecutions and are paid into the National Consolidated Fund. No asset sharing law has been enacted, but bilateral treaties as well as the Mutual Assistance in Criminal Matters Act have provisions for asset tracing, freezing and seizure between countries.

The Anti-Terrorism Act of 2002, as well as provisions of the MLFTA, criminalizes the financing of terrorism. The GOB circulates the names of suspected terrorists and terrorist organizations listed on the United Nations 1267 Sanctions Committee's Consolidated List and the list of Specially Designated Global Terrorists designated by the United States. However, there is no requirement to freeze terrorist funds or other assets of persons designated by the UN al-Qaida and Taliban Sanctions Committee. In 2008, the GOB found no evidence of terrorist financing. The GOB has not taken any specific initiatives focused on alternative remittance systems or the misuse of charitable and nonprofit entities.

Barbados has bilateral tax treaties that eliminate or reduce double taxation with the United Kingdom, Canada, Finland, Norway, Sweden, Switzerland, and the United States. The United States and the GOB ratified amendments to the bilateral tax treaty in 2004. The treaty with Canada currently allows IBCs and offshore banking profits to be repatriated to Canada tax-free after paying a much lower tax in Barbados. A Mutual Legal Assistance Treaty (MLAT) and an extradition treaty between the United States and Barbados entered into force in 2000.

Barbados is a member of the Caribbean Financial Action Task Force (CFATF), a Financial Action Task Force-style regional body, and underwent a mutual evaluation in December 2006, which was finalized in 2008. The evaluation noted deficiencies in the areas of record keeping; designated nonfinancial businesses and professions (DNFBPs); special attention for higher risk countries; and AML requirements for money/value transfer services. Barbados also is a member of the Offshore Group of Banking Supervisors, the Caribbean Regional Compliance Association, and the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. The FIU is a member of the Egmont Group. Barbados is a party to the 1988 UN Drug Convention and the UN Convention for the Suppression of the Financing of Terrorism. Barbados has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

The Government of Barbados has taken a number of steps in recent years to strengthen its anti-money laundering and counterterrorist financing legislation, and should continue to implement these reforms. The GOB should be more aggressive in conducting examinations of the financial sector and maintaining strict control over vetting and licensing of offshore entities. The GOB should devote sufficient resources to ensure the FIU, law enforcement, supervisory agencies, and prosecutorial authorities are properly staffed and have the capacity to perform their duties. The GOB should amend its legislation to allow for the seizure of suspected illegal funds at the border and to allow the freezing of funds or assets linked to terrorist financing, al-Qaida or the Taliban. Barbados should consider the adoption of civil forfeiture and asset sharing legislation. Supervision of nonprofit organizations, charities, DNFBPs, and money transfer services should be strengthened, as should information sharing between regulatory and enforcement agencies. Finally, to further enhance its legal framework against money laundering, Barbados should move expeditiously to become a party to the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Belarus

Belarus is not a regional financial center. A general lack of transparency throughout the financial sector means that assessing the level of or potential for money laundering and other financial crimes is difficult. Corruption (including embezzlement through abuse of office, taking bribes, and general abuses of power or office) and illegal narcotics trafficking are primary sources of illicit proceeds. Due

to excessively high taxes, underground markets, and the dollarization of the economy, a significant volume of foreign-currency cash transactions eludes the banking system. Shadow incomes from offshore companies, filtered through small local businesses, constitute a significant portion of foreign investment. Smuggling is prevalent. Corruption is a severe problem in Belarus, which hinders law enforcement and impedes much-needed reforms. Economic decision-making in Belarus is highly concentrated within the top levels of government. Recent decrees have further concentrated economic power into the hands of the president, granting the Presidential Administration the power to manage, dispose of, and privatize all state-owned property and to confiscate at will any plot of land for agricultural, environmental, recreational, historical, or cultural uses.

Belarus is not considered an offshore financial center, and offshore banks, shell companies, and trusts are not permitted. As of January 1, 2008, 27 banks with 368 branches comprised the banking sector. Of these, 23 were banks with foreign capital, including 7 banks with 100 percent foreign capital. There are currently eight offices of foreign banks, including those based in Germany, Latvia, Lithuania, Russia and Ukraine, and a representative office of the CIS Interstate Bank. Banks and branches have separate business units such as payment processing centers, banking service centers, and foreign exchange offices. The state-owned Belarus Bank is the largest and most influential bank in Belarus. In February 2006, the government abolished the 1997 identification requirements for all foreign currency exchange transactions at banks. Nonbank financial credit institutions have gradually closed, due to money laundering concerns and other factors.

Based on a 1996 Presidential Decree, Belarus has established one free economic zone (FEZ) in each of Belarus' six regions. The president creates FEZs upon the recommendation of the Council of Ministers and can dissolve or extend the existence of a FEZ at will. The Presidential Administration, the State Control Committee (SCC), and regional authorities supervise the activities of companies in the FEZs. According to the SCC, applying organizations are fully vetted before they are allowed to operate in an FEZ in an effort to prevent money laundering and terrorism finance. Presidential Decree 66 has tightened FEZ regulations on transaction reporting and security, including mandatory installation of video surveillance systems. A 2005 National Bank resolution changed the status of banks in the zones by removing special provisions. Banks in the zones are currently subject to all regulations that apply to banks outside the zones.

Officials have reported several cases of attempts to smuggle undeclared cash across borders. Belarus uses customs declaration forms at points of entry and exit to fulfill cross-border currency reporting requirements for both inbound and outbound currency. Upon entry into or departure from the country, travelers must declare in writing any sum over $3,000. Travelers crossing the Belarus border with sums exceeding $10,000 require permission from the National Bank to carry that amount of currency. However, the declaration system was not designed, nor is it used to detect the physical cross-border movement of currency and bearer negotiable instruments to prevent and interdict bulk cash smuggling for money laundering and terrorist financing purposes. Individuals may import or export securities certificates denominated in foreign currencies and payment instruments in foreign currencies without any limitations on the amount, and without the need to declare them in writing to the customs authorities. Customs authorities do not store information on declarations that they consider suspicious and are unable to apply sanctions against persons moving funds cross-border on the basis of suspicion of money laundering or terrorist financing.

The Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG), a Financial Action Task Force (FATF)-style regional body, evaluated the anti-money laundering and counterterrorist financing (AML/CTF) regime of Belarus in July 2008. The EAG adopted the mutual evaluation report (MER) at the December 2008 plenary meeting. The major deficiencies outlined in the MER focused on the lack of adequate customer due diligence (CDD) requirements, including allowing electronic cash accounts in fictitious names , no clear requirement to perform CDD on establishing business relations with a customer in the banking, insurance and securities sectors; no

requirement for CDD for legal entities below ($300,000) threshold; no affirmative obligation to identify beneficial ownership in the banking sector, and no beneficial ownership or ongoing monitoring requirements for other sectors; and lack of effective regulation and supervision for correspondent accounts and designated nonfinancial businesses and professions (DNFBPs); inadequate record keeping requirements; inadequate wire transfer identifier requirements; and shortcomings in the Belarusian cross-border cash declaration regime.

By law, only licensed banks and the postal service can conduct money transfers. The government does not acknowledge alternative remittance systems and allows currency exchange only through licensed currency exchange kiosks. The Department of Humanitarian Assistance in the Presidential Administration has registered all charities. Presidential Decree 24, passed in 2003, requires all organizations and individuals receiving charity assistance, including assistance provided by foreign states, international organizations and individuals, to open charity accounts in a local bank.

Belarus' "Law on Measures to Prevent the Laundering of Illegally Acquired Proceeds" (AML Law), adopted in 2000 and amended in 2005, establishes the legal and organizational framework to prevent money laundering and terrorist financing. The AML/CTF law does not fully incorporate the requirements of the Vienna and Palermo Conventions (e.g., acquisition possession or use are not covered, nor are indirect proceeds). Belarus criminalizes self-laundering, but restricts the self-laundering offense to cases that involve using the illicit proceeds to carry out entrepreneurial or other business activities. Belarus also criminalizes the financing of terrorism. Although Belarus has adopted an all crimes approach to money laundering predicates, with some exceptions for tax evasion crimes, it does not criminalize insider trading and market manipulation, and therefore does not meet FATF requirements for the minimum list of predicate offenses. A money laundering conviction does not require conviction of the predicate offense. Legal entities are not criminally liable and there also is no administrative liability of r legal entities for money laundering. However, if a legal entity aids an organized group or criminal organization or is created with funds of an organized group or criminal group, it can be liquidated by the Supreme Court of Belarus and its assets seized by the state. The criminal code provides adequate sanctions for individuals convicted of money laundering, including fines and incarceration for two-1- years. The law defines "illegally acquired proceeds" as currency, securities or other assets, including real and intellectual property rights, obtained in violation of the law.

Financial institutions are obligated to report suspicious transactions regardless of value, and large value transactions, for which the reporting threshold for individual financial transactions is approximately $27,000 and for corporate transactions is approximately $270,000. In Belarus, these reporting obligations attach to transfers that are subject to special monitoring. Specifically, transactions subject to special monitoring include: transactions whose suspected purpose is money laundering or terrorist financing; cases where the person performing the transaction is a known terrorist or controlled by a known terrorist; cases in which the person performing the transaction is from a state that does not cooperate internationally to prevent money laundering and terrorist financing; and transactions exceeding the currency reporting threshold that involve cash, property, securities, loans or remittances. Financial institutions conducting such transfers are required to disclose to the FIU—the Department of Financial Monitoring (DFM)—within one business day the identity of the individuals and businesses ordering the transaction or the person on whose behalf the transaction is being placed, information about the beneficiary of a transaction, and account information and document details used in the transaction. If the total value of transactions conducted in one month exceeds set thresholds and there is reasonable evidence to suggest that the transactions are related, then all the transaction activity must be reported. Banks that violate the law face fines of up to one percent of their registered capital and suspension of their licenses for up to one year. However, the AML Law exempts most government transactions and those sanctioned by the President from

reporting requirements (extraordinary inspection). The government has used the AML Law as a pretext for preventing several pro-democracy NGOs from receiving foreign assistance.

The AML Law authorizes the following government bodies to monitor financial transactions for the purpose of preventing money laundering: the State Control Committee (SCC); DFM; the Securities Committee; the Ministry of Finance; the Ministry of Justice; the Ministry of Communications and Information; the Ministry of Sports and Tourism; the Committee on Land Resources; the Ministry on Taxes and Duties (MTD); and other state bodies. The MTD also provides oversight and has released binding regulations on its subject institutions. Under the SCC, the Department of Financial Investigations, in conjunction with the Prosecutor General's Office, has the legal authority to investigate suspicious financial transactions and examine the internal rules and enforcement mechanisms of any financial institution.

In January 2005, the President signed a decree on the regulation of the gaming sector, imposing stricter tax regulations on owners of gaming businesses. In addition, a provision intended to combat money laundering requires those participating in gaming activities to produce identification to receive winnings. However, casinos do not need to address AML/CTF issues before receiving operating licenses, and the system for supervising and applying sanctions for noncompliance with AML/CTF requirements is not effective. Belarus has similar shortcomings with the other DNFBPs: there is little effective monitoring for compliance with AML/CTF measures for most of these sectors, and accountants lack a supervisory agency—even a self-regulating organization—so they completely lack supervision and monitoring altogether. Across sectors, there is no clear customer identification requirement for DNFBPs at the establishment of the business relationship, there are no beneficial ownership identification requirements, and exceptions in the reporting requirements mean that there may be times that DNFBPs do not perform client identification measures even when they suspect the client of involvement in money laundering or terrorist financing. These sectors also lack the legal obligation to execute enhanced CDD measures for high-risk clients. Likewise, Belarus has no requirements for these sectors to obtain information from the customer regarding his or her source of funds or the expected purpose of the business relationship. The MER notes an overall lack of implementation across these sectors, in particular, the absence of effectiveness in the gaming sector, as well as with regard to dealers in precious metals and stones.

In 2003, Belarus established the DFM as its financial intelligence unit (FIU). Although it is an autonomous unit within the State Control Committee of Belarus with the rights of a legal entity, it does not have an independent budget and cannot independently hire staff. As the primary government agency responsible for gathering, monitoring and disseminating financial intelligence, the DFM analyzes financial information for evidence of money laundering and forwards it to law enforcement officials for prosecution. The DFM also has the power to penalize those who violate money laundering laws and suspend the financial operations of any company suspected of money laundering or financing terrorism. The DFM cooperates with counterparts in foreign states and with international organizations to combat money laundering, and since 2007 it is a member of the Egmont Group. The DFM also has the authority to initiate its own investigations. In 2007 the DFM received and analyzed 269,701 suspicious transaction reports (STRs) and forwarded 2,088 reports to law enforcement and control authorities.

The DFM has noted that there is increased interest by law enforcement in the FIU's work. Belarusian legislation provides for broad seizure powers for law enforcement to identify and trace assets. The Criminal Code provides for asset forfeiture for all serious offenses, including money laundering. Seizure of assets from third parties appears possible but is not specifically codified. The seizure of funds or assets held in a bank requires a court decision, a decree issued by a body of inquiry or pre-trial investigation, or a decision by the tax authorities.

Belarus has focused on targets beyond money laundering. In June 2007 Parliament passed Criminal Code amendments to toughen penalties for various offenses by officials, including larceny through abuse of office, embezzlement, and legalization of assets illegally obtained. In July 2007, President Lukashenko issued an edict mandating the formation of specialized departments within prosecutors' offices, police stations and the KGB to fight against corruption and organized crime. Despite recent legislation, corruption remains a serious obstacle to enforcing laws dealing with financial crimes.

Belarus has made an effort to ensure cooperation and coordination between state bodies through the Interdepartmental Working Group established specifically to address AML/CTF issues. This Working Group includes representatives of the Prosecutor's office, the National Bank, MTD, State Security Committee, Department of Financial Investigation, and the DFM. The Director of the DFM serves as the head of this Group.

Terrorism is a crime in Belarus and the willful provision or collection of funds in support of terrorism by nationals of Belarus or persons in its territory constitutes participation in terrorism by aiding and abetting. Article 290-1 of the Criminal Code explicitly criminalizes terrorist financing. However, the law does not criminalize indirect provision of money for purposes of terrorist financing and does not criminalize provision of funds for a terrorist organization or an individual terrorist, if the funds are not intended for a specific act of terrorism. The Criminal Code also does not criminalize the financing of theft of nuclear materials for terrorist purposes. Legal entities are not criminally liable for terrorist financing, but organizations engaged in the financing of terrorism may be liquidated by decision of the Supreme Court upon indictment by the General Prosecutor. In December 2005, the Parliament amended the Criminal Code to stiffen the penalty for the financing of terrorism The amendments explicitly define terrorist activities and terrorism finance and carry an eight to twelve year prison sentence for those found guilty of sponsoring terrorism. In February 2006, the Interior Ministry announced the establishment of a new counterterrorism department within its Main Office against Organized Crime and Corruption.

Belarus does not have an adequate system in place to freeze without delay terrorist assets. The AML/CTF (Article 5) requires financial institutions and DNFBPs to suspend a financial transaction if one of its participants is a person suspected of being involved in terrorist activities or controlled by terrorists. The National Bank provides banks with the State Security Committee's lists of persons suspected of being involved in terrorist activities or controlled by persons engaged in terrorism—including persons on the United Nations Security Council Resolution (UNSCR) 1267 Sanctions Committee's consolidated list—and has given banks and nonbank credit institutions an instruction on the procedure for freezing funds. DNFBPs do not receive the terrorism lists and have little awareness of freezing requirements. In addition, the AML/CTF law (Article 11) also authorizes the Financial Monitoring Department to suspend a transaction for up to five days, after which time it must decide either to report the information to law enforcement, which can attach the funds, or resume the transactions. In accordance with a resolution passed in March 2006, the Belarusian KGB compiled a list of 221 individuals suspected of participation in terrorism, which the National Bank distributed to all domestic banks. Belarus has no procedures in place for reviewing requests to remove persons from the list or for unfreezing the funds of persons to whom the freezing mechanism was accidentally applied.

Belarus is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. Belarus has signed bilateral treaties on law enforcement cooperation with Afghanistan, Bulgaria, India, Latvia, Lithuania, the People's Republic of China, Poland, Romania, Syria, Turkey, the United Kingdom, and Vietnam. In September 2006, Belarus signed an AML agreement with the People's Bank of China. The United States and Belarus do not have a mutual legal assistance agreement in place. Belarus is a member of the EAG. The DFM is a member of the

Egmont Group. Belarus is ranked number 151 out of 180 territories listed in Transparency International's 2008 International Corruption Perception Index.

The Government of Belarus (GOB) has taken steps to construct a legal and regulatory framework to fight money laundering and terrorist financing. It should also focus on the implementation of the law by law enforcement, increasing the investigation and prosecution of money laundering and terrorist financing offenses. This could be accomplished through training and outreach by the FIU and other regulators. Belarus should increase the transparency of its business, finance, and banking sectors. Belarus' AML legislation should be further amended to comport with international standards and to provide for more transparency and accountability. The GOB should, for example, extend the application of its current AML legislation to cover the governmental transactions that are currently exempted under the law, and ensure that the regulations and guidance provided by the National Bank and other regulators are legally binding. Similarly, the National Bank should be given the authority to carry out its responsibilities, and not be subject to influence by the Presidential Administration. The GOB should also bring the nonfinancial sectors under the same AML/CTF requirements that it imposes on the financial sector, and ensure resources for supervision, monitoring and a sanctions regime for noncompliance. The GOB should implement strict regulation on its industries operating abroad and on those operating within the FEZ areas. The GOB needs to reinstate the identification requirement for foreign currency exchange transactions, and reconsider the relationships it wishes to foster with state sponsors of terrorism. Belarus should continue to hone its guidance and enforcement of suspicious transaction reporting and provide adequate staff, tools, training and financial resources to its FIU so that it can operate effectively, especially with the increased attention and reporting that the DFM has generated of late. The GOB must work to further improve the coordination between agencies responsible for enforcing AML measures. The GOB also needs to take steps to ensure that the AML framework operates more objectively and less as a political tool. The GOB should take serious steps to combat corruption in commerce and government.

Belgium

Belgium's banking industry is of medium size, with assets of over $2 trillion dollars in 2008. Illicit funds, formerly consisting mostly of narcotics-trafficking proceeds, now derive mainly from financial fraud, including tax fraud. Other noteworthy predicate offenses include trafficking in persons and in diamonds, due to Belgium's active diamond industry, as well as in other goods. Authorities note that criminals are increasing their use of remittance transactions and shell companies, and misuse of the nonfinancial sectors, in particular lawyers, real estate and nonprofit organizations to launder money.

Strong legislative and oversight provisions are in place in the formal financial sector to combat money laundering and terrorist financing. Belgium criminalized money laundering with the Law of 11 January 1993, On Preventing Use of the Financial System for Purposes of Money Laundering. Additional laws expanded the scope of the legislation: the Law of 22 March 1993, On the Legal Status and Supervision of Credit Institutions; and the Law of 6 April 1995, On Secondary Markets, On Legal Status and Supervision of Investment Firms, On Intermediaries and Investment Advisors. These laws mandate the customer due diligence and reporting requirements that apply to banks and the formal financial sector as well as nonfinancial businesses and professions, including estate agents, private security firms, funds transporters, diamond merchants, notaries, bailiffs, auditors, chartered accountants, tax advisors, certified accountants, surveyors and casinos. Article 505 of the Penal Code sets penalties of up to five years of imprisonment for money laundering convictions. Any unlawful activity may serve as the predicate offense.

The Law of 12 January 2004 amended Belgian domestic legislation by making it applicable to attorneys and broadening the scope of money laundering predicate offenses beyond drug trafficking to include the financing of terrorist acts or organizations. The Belgian bar association challenged this law

and brought it to the Court of Arbitration, which referred the challenge to the European Court of Justice. The bar argued that the Second EU Directive, which served as the basis for this law, violates the right to a fair trial, because the reporting obligations prejudice lawyers against fully and independently representing their clients. In October 2008, the European Commission referred Belgium to the European Court of Justice over non-implementation of the Third Money Laundering Directive, which requires members to update their AML regimes to comport with the most up-to-date standards, particularly with regard to regulation and terrorism financing.

Belgium is currently working to address the deficiencies described in the 2005 Financial Action Task Force (FATF) mutual evaluation report (MER), including due diligence and regulation requirements for designated nonfinancial businesses and professions, licensing or registration of businesses providing money or value transfer services, allocation of adequate resources to the authorities charged with combating financial crimes, elimination of bearer bonds, development of an independent authority to freeze assets, and implementation of a system to monitor cross-border currency movements.

Authorities believe that 3,500 phone shops—small businesses where customers can make inexpensive phone calls and access the internet—may be operating in Belgium. Only an estimated one-quarter of these shops are formally licensed, and Belgian authorities are considering enforcing a stricter licensing regime. Some Brussels communes have also proposed heavy taxes on these types of shops in an effort to dissuade illegitimate commerce. Since 2004, Belgian police made a series of raids on "phone shops." In some phone shops, authorities uncovered money laundering operations and hawala-type banking activities. In 2006 and 2007 raids in some locations uncovered numerous counterfeit phone cards in addition to evidence of money laundering activities. Authorities have closed more than 200 such shops since 2004, and estimate that the Belgian state loses up to $256 million in tax revenue each year through tax evasion by these businesses. Authorities report that phone shops often declare bankruptcy and later reopen under new management, making it difficult for officials to trace ownership and collect tax revenues. In 2007, the cities of Antwerp and Gent also increased enforcement activities against such phone shops.

Despite some diffusion in recent years, Belgium continues as the world's diamond-trading center. Fully 90 percent of the world's crude diamonds and 50 percent of cut diamonds pass through Belgium. The Government of Belgium (GOB) recognizes the particular importance of the diamond industry, as well as the potential vulnerabilities it presents to the financial sector. The GOB has distributed typologies outlining its experiences in pursuing money laundering cases involving the diamond trade, especially those involving the trafficking of African conflict diamonds. The Kimberley certification process has introduced much-needed transparency into the global diamond trade. A regulation approved by a Royal Decree dated October 22, 2006 contains a detailed description of the obligations that diamond dealers must observe. This regulation primarily deals with the different aspects of the client's identification, including the identification of 'non-face-to-face' operations and of the beneficial owner, customer due diligence and obligations regarding the internal organization. Belgium's robust diamond industry presents special challenges for law enforcement, but authorities have transmitted a number of cases relating to diamonds to the public prosecutor, and they monitor the sector closely in cooperation with local police and diamond industry officials.

The Belgian financial institutions are supervised by the Belgian Banking and Finance Commission (CBFA) supervises financial institutions, exchange houses, stock brokerages, and insurance companies. The Belgian Gaming Commission oversees casinos. Belgian law mandates reporting of suspicious transactions by a wide variety of financial institutions and nonfinancial entities, including notaries, accountants, bailiffs, real estate agents, casinos, cash transporters, external tax consultants, certified accountant-tax experts, and lawyers. Lawyers in particular do not consistently comply with reporting requirements.

Financial institutions must comply with "know your customer" principles, regardless of transaction amount. Institutions must maintain records on the identities of clients engaged in transactions that are considered suspicious or that involve an amount equal to or greater than 10,000 euros (approximately $12,500) as well as retain records of suspicious transactions reported to the FIU for at least five years.

Financial institutions or other entities with reporting requirements are liable for illegal activities occurring under their control. Financial institutions must train their personnel in the detection and handling of suspicious transactions that could be linked to money laundering. Failure to comply with the anti-money laundering legislation, including failure to report, carries a fine of up to $1.72 million.

Money laundering legislation imposes restrictions on cash payments for real estate. Purchasers may not use cash for amounts exceeding 10 percent of the purchase price or approximately $18,750, whichever is lower. Cash payments over $25,000 for goods are also illegal.

Belgium had long permitted the issuance of bearer bonds ("titres au porteur"), widely used to transfer wealth between generations and to avoid taxes. As of January 1, 2008, companies may no longer issues bearer bonds, although bearer bonds issued before that date are still valid, as are non-Belgian bearer bonds. Bearer shares are permitted for individuals as well as for banks and companies.

In Belgium, the Royal decree of 5 October 2006 on measures to control cross-border transportation of cash came into force on June 15, 2007. The Royal decree stipulates the obligation to declare transportation of currency worth 10,000 euros or more in cash entering or leaving the EU/Belgium.

In cases of a failure to declare, or if there is a suspicion that the cash declared originates from illegal activities or is intended to finance such activities, the Belgian Customs and Excise administration will confiscate the cash for up to 14 days and send a report to the financial intelligence unit (FIU). The FIU examines all the declarations submitted and Customs reports filed. Since June 2007, Belgian Customs has received information about 4.5 million euros in cash passing through Zaventem International airport. To date, Belgian Customs has confiscated 670,000 euros and filed 196 reports with the FIU.

Belgian officials are working to increase transparency in the nonprofit sector through better enforcement of registration and reporting procedures. Nonprofit organizations must register, furnish copies of their statutes and membership lists, provide minutes from council meetings, and file budget reports.

The Belgian financial intelligence unit, known in French as the Cellule de Traitement des Informations Financières and in Flemish as Cel voor Financiële Informatieverwerking (CTIF-CFI), was created by a Royal Decree issued on June 11, 1993. The FIU is an autonomous and independent public administrative authority supervised by the Ministries of Justice and Finance. Institutions and persons subject to the reporting obligations fund the FIU. Although these contributions are compulsory, the contributing entities do not exercise any formal control over the FIU. CTIF-CFI's primary mission is to receive, analyze, and disseminate all suspicious transaction reports (STRs) submitted by obliged entities. Operating as a filter between obligated entities and judicial authorities, CTIF-CFI reports possible money laundering or terrorist financing transactions to the public prosecutor. The financial sector cooperates actively with CTIF-CFI to guard against illegal activity. Employees and representatives of institutions who report transactions to CTIF-CFI in good faith are exempt from civil, penal, or disciplinary actions. Legislation also exists to protect witnesses, including bank employees, who report suspicions of money laundering or who come forward with information about money laundering crimes. Belgian officials have imposed sanctions on institutions or individuals that knowingly permitted illegal activities to occur. CTIF-CFI also acts as the supervisory body for professions not supervised by CBFA or other authorities. CTIF-CFI has also been very active in analyzing the diamond industry and working to eliminate its potential for money laundering and terrorist financing.

The FIU is composed of financial experts, including three magistrates (public prosecutors), appointed by the King, who serve six-year renewable terms. A magistrate presides over the body. In addition to administrative and legal support, the investigative department consists of inspectors/analysts. There are also liaisons that maintain contact with the various law enforcement agencies in Belgium, including three police officers, one customs officer, and one officer of the Belgian intelligence service.

From its founding in 1993 until the end of 2007, CTIF-CFI received 127,293 disclosures and opened a total of 30,223 individual case files (numerous disclosures may be linked to a single case). Of these, the FIU has transmitted 8,310 cases to the public prosecutor aggregating approximately $16.5 billion. In 2007, the FIU received 12,830 disclosures, opened 4,927 new cases, and transmitted 1,166 cases to the public prosecutor, up from 912 cases transmitted in 2006. Reports from credit institutions comprise about 81 percent of disclosures on files transmitted to the federal prosecutor. Foreign exchange offices and foreign counterpart units accounted for an additional 12 percent of the files transmitted, with notaries, casinos, and other entities also reporting. The files concerning serious and organized tax fraud represented 36.7 percent of the total number of cases in 2007, while cases regarding terrorism and terrorist finance represent 7 percent of the total amount (up from 6 percent in 2006). Belgian statistics show that from the start of its activities until the end of 2007, the FIU reported 175 cases regarding terrorism or terrorist financing to the judicial authorities. Thirty-two of theses cases were reported in 2007.

Since the creation of CTIF-CFI in 1993, Belgian courts and tribunals have pronounced sentences in at least 1,046 of the 8,310 cases transmitted to the Federal Prosecutor (some of these convictions are still under appeal). From 1993-2007, the conviction rate was 11.4 percent. To date, Belgian courts have convicted 2,060 individuals for money laundering on the basis of cases forwarded by the FIU, yielding combined total sentences of 3,568 years. Although five years imprisonment is the maximum sentence for money laundering, the length of the sentence may increase if the financial crime is compounded by another type of crime such as drug trafficking. The cumulative fines levied for money laundering total approximately $91 million. Belgian authorities have confiscated more than $788 million connected with money laundering crimes. The majority of convictions related to money laundering are based upon disclosures made by the financial institutions and others to CTIF-CFI.

As with Belgium's FIU, the federal police must transmit suspected money laundering cases to the public prosecutor. In 2006 the federal police referred a total of 2,241 individuals to the public prosecutor for various crimes. More than 20 percent of these (450 individual cases) involved money laundering, fraud, and corruption, and 28 percent involved narcotics. The federal police established a special bureau to combat VAT fraud shortly after 2001, when estimates of lost revenue topped $1.4 billion. In 2007, 57.3 percent of all cases reported to the Public Prosecutor involved VAT carousel fraud. The federal police and the specialized services of the Central Office for the Fight against Organized Economic and Financial Crimes utilize a number of tactics to uncover money laundering operations, including investigating significant capital injections into businesses, examining suspicious real estate transactions, and conducting random searches at all international airports. According to the FATF MER, prosecutorial authorities have the necessary power to carry out their functions; however, in places or at times, the prosecutors and police seem to lack resources to properly perform their AML/CTF duties.

Belgium has created a sophisticated and comprehensive confiscation and seizure regime, encompassing the Central Office for Seizure and Confiscation (COSC), operating under the auspices of the Ministry of Justice. The COSC ensures that authorities execute confiscations and seizures smoothly and efficiently in accordance with the law. Belgian law requires a judicial order to execute confiscations and seizures, and allows civil as well as criminal forfeiture of assets. A law passed in July 2006 allows for the possibility, on a reciprocal basis, of the sharing of seized assets from serious crimes, including those related to narcotics, with affected countries.

Seizures in Belgium can be direct or indirect. Direct seizures involve the seizure of items linked directly to a crime. Indirect seizures are "seizures by equivalence," usually of homes, cars, jewels and other items not directly linked to the crime in question. Belgian authorities attempt to sell confiscated items such as cars, computers, and cell phones soon after confiscation in order to minimize the loss of the market value of the goods over time. If a suspect is later found innocent, he or she receives the cash equivalent of the item(s) sold, plus accrued interest. Money from seizures and from the sale of seized goods is deposited in the Belgian Treasury. COSC has a commercial account for the deposit of confiscated funds. As of October 2007, the fund held more than $165 million. COSC also maintains safe deposit boxes for the storage of high value items, such as jewelry. Belgium has a verification program to check legal records of suspects to whom the authorities will return seized assets. If the person owes taxes or has overdue fines, COSC can ensure that the Belgian government is paid before proceeds are returned. According the COSC, information concerning the value of seizures is not available publicly.

In January 2004, the Belgian legislature passed domestic legislation criminalizing terrorist acts and material support (including financial support) for terrorist acts, allowing judicial freezes on terrorist assets. The law implemented eight of FATF's Special Recommendations, including prohibiting the provision of material support to terrorists groups by nonprofit organizations. Article 140 of the Penal Code criminalizes participation in the activity of a terrorist group, and Article 141 criminalizes the provision of material resources, including financial assistance, to terrorist groups and carries a penalty of five to ten years' imprisonment.

Under Belgium's 1993 anti-money laundering and counterterrorist finance (AML/CTF) law (amended in 2004), bank accounts can be frozen on a case-by-case basis if there is sufficient evidence that a money laundering crime has been committed. The FIU has the legal authority to suspend a transaction for a period of up to two working days in order to complete its analysis. If criminal evidence exists, the FIU forwards the case to the public prosecutor. In 2006, CTIF-CFI temporarily froze assets in 41 cases, representing approximately $220 million. To date, there are no figures for 2007 or 2008.

Under the January 2004 law, the Ministry of Justice can freeze assets related to terrorist crimes. However, in order for an act to constitute a criminal offense, authorities must demonstrate that the support was given with the knowledge that it would contribute to the commission of a crime by the terrorist group. Since the law does not establish a national capacity for designating foreign terrorist organizations, authorities must demonstrate in each case that the group that was lent support actually constitutes a terrorist group.

In Belgium, the Ministry of Finance can administratively freeze assets of individuals and entities associated with al-Qaeda, the Taliban and Usama Bin Laden on the United Nations 1267 Sanctions Committee's consolidated list and/or those covered by an EU asset freeze regulation. Seized assets are transferred to the Ministry of Finance. If an entity appears on the UN 1267 Sanctions Committee's consolidated list, the GOB can pass a ministerial decree to freeze assets in order to comply with the UN requirement. Assets of entities appearing on the EU list are automatically subject to a freeze without additional legislative or executive procedures. Belgium is working on legislation to permit the administrative freeze of terrorist assets in the absence of a judicial order or UN or EU designation.

CTIF-CFI was a founding member of the Egmont Group and headed the Secretariat from 2005 to 2006. Belgium's FIU shares information with its European colleagues. Belgium is also a cooperative and reliable partner in law enforcement efforts. The federal police enjoy good cross-border cooperation with other police and investigative services in neighboring countries. Belgium does not require an international treaty as a prerequisite to lending mutual assistance in criminal cases.

Belgium is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Belgium also ratified the UN Convention against Corruption in September 2008. A mutual legal assistance treaty

(MLAT) between Belgium and the United States has been in force since 2000. Belgium and the United States have since signed a bilateral instruments amending and supplementing this treaty, in implementation of the U.S.-EU Extradition and Mutual Legal Assistance Agreements.

The Government of Belgium's (GOB's) continuing work implementing the FATF recommendations complements an already solid anti-money laundering regime and a clear official commitment to fighting against financial crimes, including the financing of terrorism. Belgium should also prohibit all bearer shares. Belgium should continue to work through proposed legislation that pursues tougher and faster independent asset-freezing capability as well as the optimal disposition of seized assets. Belgium should continue its efforts to uncover, investigate, and prosecute illegal banking operations, as well as the informal financial sector and nonbank financial institutions. The GOB should strengthen enforcement of reporting requirements by some nonfinancial entities in Belgium, in particular lawyers and notaries. To be even more effective in its efforts, Belgium may need to devote more resources, including investigative personnel, to police, prosecutors and key Belgian agencies that work on money laundering, terrorist financing, and other financial crimes.

Belize

Belize is not a major regional financial center. In an attempt to diversify Belize's economic activities, authorities have encouraged the growth of offshore financial activities that are vulnerable to money laundering. Belize has pegged the Belizean dollar to the U.S. dollar and continues to offer financial and corporate services to nonresidents in its offshore financial sector. Belizean officials suspect that money laundering occurs primarily within that sector. Money laundering, primarily related to narcotics trafficking, and contraband smuggling, is suspected to occur through onshore banks operating in Belize. There is no evidence to indicate that money laundering proceeds are primarily controlled by local drug trafficking organizations organized criminals or terrorist groups. The vulnerability created by the government's lack of supervision of its offshore sector is exacerbated by its the lack of supervision of the gaming sector, including Internet gaming facilities, and the refusal of the Government of Belize (GPB) to fund its financial intelligence unit.

Offshore banks, international business companies, and trusts are authorized to operate from within Belize, although shell banks are prohibited within the jurisdiction. The Offshore Banking Act, 1996 governs activities of Belize's offshore banks. By law, offshore banks cannot serve customers who are citizens or legal residents of Belize. To legally operate, all offshore banks must be licensed by the Central Bank and be registered with the international business companies (IBCs) registry. Before the Central Bank issues the license, the Central Bank must verify shareholders' and directors' backgrounds, ensure the adequacy of capital, and review the bank's business plan. The legislation governing the licensing of offshore banks does not permit nominee directors.

Presently, there are eight licensed offshore banks, approximately 32,800 active registered IBCs, one licensed offshore insurance company, one mutual fund company, and 30 trust companies and agents operating in Belize. Neither offshore banks nor onshore banks are permitted to issue bearer shares. Only the Central Bank of Belize and authorized dealers/depositories (i.e., commercial banks and casas de cambio) may deal in foreign currencies. Local money exchange houses, which were suspected of money laundering, were closed effective July 2005. Internet gaming is regulated by a Gaming Control Board, which is guided by the Gaming Control Act. There is one licensed internet gaming site, but there are an undisclosed number of Internet gaming sites illegally operating from within the country. Reportedly, there are no offshore casinos.

The International Business Companies Act of 1990 and its 1995 and 1999 amendments govern the operation of IBCs. The 1999 amendment to the Act allows IBCs to operate as banks and insurance companies. The International Financial Services Commission regulates the nonbanking sector for the provision of international financial services. All IBCs must be registered. Although nonbank IBCs are

allowed to issue bearer shares, the registered agents of such companies must know the identity of the beneficial owners of the bearer shares. Belize's legislation allows for the appointment of nominee directors of nonbank IBCs. The legislation for trust companies, the Belize Trust Act, 1992, is not as stringent as the legislation for other offshore financial services and does not preclude the appointment of nominee trustees.

There is one free trade zone presently operating in Belize, at the border with Southern Mexico. There are also designated free trade zones in Punta Gorda, Belize City, and Benque Viejo, but they are not operational. Data Pro Ltd., formerly primarily engaged in internet gaming, was sold to Belize Telemedia Limited and is now International Communications and Services Limited. It is designated as an Export Processing Zone (EPZ) and is regulated in accordance with the EPZ Act. There are presently 59 EPZ's in Belize. Commercial free zone (CFZ) businesses are allowed to conduct business within the confines of the CFZ, provided they have been approved by the Commercial Free Zone Management Agency (CFZMA) to engage in business activities. All merchandise, articles, or other goods entering the CFZ for commercial purposes are exempted from the national customs regime. However, any trade with the national customs territory of Belize is subject to the national Customs and Excise law. The CFZMA, in collaboration with the Customs Department and the Central Bank of Belize, monitors the operations of CFZ business activities. There is no indication the CFZ is presently being used in trade-based money laundering schemes or by financiers of terrorism. The incidents involving developments in the CFZ have largely been related to counterfeit goods and more recently, pharmaceuticals such as ephedrine and pseudo-ephedrine.

Alternative remittance systems are illegal in Belize. However, Belizean authorities acknowledge the existence and use of indigenous alternative remittance systems that bypass, in whole or part, financial institutions, and these systems have not yet been deterred through fines or criminal prosecution. Belizean customs authorities monitor such activities at the borders with Mexico and Guatemala; however, no domestic investigations have been undertaken.

Allegedly, there is a significant black market for smuggled goods in Belize. However, there is no evidence to indicate that the smuggled goods are significantly funded by narcotics proceeds, or evidence to indicate significant narcotic-related money laundering. The funds generated from contraband are undetermined.

The Money Laundering (Prevention) Act (MLPA), in force since 1996 and amended in 2002, criminalizes money laundering related to many serious crimes, including drug trafficking, forgery, terrorism, blackmail, arms trafficking, kidnapping, fraud, illegal deposit taking, false accounting, counterfeiting, extortion, robbery, and theft. The minimum penalty for a money laundering offense as defined by the MLPA is three years imprisonment. Other legislation to combat money laundering includes the Money Laundering Prevention Guidance Notes; the Financial Intelligence Unit Act, 2002; the Misuse of Drugs Act; The International Financial Services Practitioners Regulations (Code of Conduct), 2001 (IFSPR); Money Laundering Prevention Regulations 1998 (MLPR); and the Offshore Banking Act, 2000, renamed the International Banking Act, 2002 (IBA).

The Central Bank of Belize supervises and examines financial institutions for compliance with anti-money laundering and counterterrorist financing laws and regulations. The banking regulations governing offshore banks are different from the domestic banking regulations in terms of capital and operational requirements. Nevertheless, all licensed financial institutions in Belize (onshore and offshore) are governed by the same legislation and must adhere to the same anti-money laundering and counterterrorist financing requirements. Government of Belize (GOB) officials have reported an increase in financial crimes, such as bank fraud, cashing of forged checks, suspicious transactions, and counterfeit Belizean and United States currency. The Central Bank of Belize continues to engage in public awareness activities and conduct training sessions related to counterfeit currency.

The Central Bank issued Supporting Regulations and Guidance Notes in 1998. Licensed banks and financial institutions are required to establish due diligence ("know-your-customer") provisions, monitor their customers' activities and report any suspicious transaction to the financial intelligence unit (FIU) of Belize. Belize law obligates banks and other financial institutions to maintain business transactions records for at least five years when the transactions are complex, unusual, or large. Money laundering controls are also applicable to nonbank financial institutions, such as exchange houses, insurance companies, lawyers, accountants and the securities sector, which are regulated by the International Financial Services Commission. Financial institution employees are exempt from civil, criminal, or administrative liability for cooperating with regulators and law enforcement authorities in investigating money laundering or other financial crimes. Belize does have bank secrecy legislation that prevents disclosure of client and ownership information but information can be made available at the request of the courts. These bank secrecy provisions significantly hamper the GOB's ability to assist other governments in mutual legal assistance requests for financial records.

The reporting of all cross-border currency movement is mandatory. All individuals entering or departing Belize with more than $10,000 in cash or negotiable instruments are required to file a declaration with the authorities at Customs, the Central Bank and the FIU.

The FIU of Belize, established in 2002, is an independent agency presently housed at the Central Bank. Although it is a member of the Egmont Group, current laws do not provide for the funding of the FIU, and the FIU has to apply to the Ministry of Finance for funds. Due to financial constraints, the FIU is not adequately staffed and existing personnel lack sufficient training and experience. Currently, the FIU has a seven member staff: a director, a legal officer, an investigator, a financial examiner, an office manager, an office assistant, and a secretary. Historically, there has been a lack of coordination between the FIU and the Director of Public Prosecutions, resulting in the FIU attempting to bring its own cases, which are often dismissed from court.

The Director of the Public Prosecutions Office and the Belizean Police Department are responsible for investigating all crimes. However, the FIU also has administrative, prosecutorial and investigative responsibilities for financial crimes, such as money laundering and terrorist financing. The anti-money laundering regime in Belize remains relatively ineffective. The FIU received 49 suspicious transaction reports (STRs) during 2008. Fourteen became the subject of investigations. The FIU usually sends queries to the Securities and Exchange Commission and the Financial Crimes Enforcement Network (FinCEN) in the United States and investigations remain open until responses are received. In 2007, there were press reports indicating a possible money laundering scheme by a former public official, but no subsequent investigation was conducted. In 2008, relatives of high ranking government officials were allegedly linked to a money laundering scheme spanning offshore accounts in several countries including Belize. In December 2008, the FIU dropped charges against two of Belize's most prominent banks, the Belize Bank and First Caribbean International Bank—a Canadian controlled bank. The banks had faced charges related to several millions in "suspicious transactions" they were accused of failing to report. The official reason given for dropping the charges was because foreign correspondent banks were discussing severing ties with local banks, threatening to cause a possible collapse and a destabilization of the country's financial sector. The banks are to fund an electronic reporting system for the country, and fund refurbishment of two parks, equal to a monetary penalty of $300,000. The DPP needs to designate, and specially train, attorneys to pursue money laundering charges.

Although the FIU has access to records and databanks of other GOB entities and financial institutions, there are no formal mechanisms for the sharing of information with domestic regulatory and law enforcement agencies. However, the FIU is empowered to share information with FIUs in other countries. On several occasions, the FIU has cooperated with the United States.

Belizean law makes no distinctions between civil and criminal forfeitures. All forfeitures resulting from money laundering or terrorist financing are treated as criminal forfeitures. The banking community cooperates fully with enforcement efforts to trace funds and seize assets. The FIU and the Belize Police Department are the entities responsible for tracing, seizing and freezing assets and the Ministry of Finance can also confiscate frozen assets. With prior court approval, Belizean authorities have the power to identify, freeze, and seize assets related to money laundering or terrorist financing. Currently, the GOB's legislation does not specify the length of time assets can be frozen. There are no limitations to the kinds of property that may be seized, and any property—tangible or intangible—that may be related to a crime or is shown to constitute the proceeds of a crime, including legitimate businesses, may be seized. However, Belizean law enforcement lacks the resources necessary to effectively trace and seize assets.

GOB authorities are considering the enactment of a Proceeds of Crime law, which will address the seizure or forfeiture of assets of narcotics traffickers, financiers of terrorism, or organized crime. Currently, the GOB is not engaged in any bilateral or multilateral negotiations with other governments to enhance asset tracing and seizure. However, the GOB cooperates with the efforts of foreign governments to trace or seize assets related to financial crimes.

Belize criminalized terrorist financing via amendments to its anti-money laundering legislation, The Money Laundering (Prevention) (Amendment) Act, 2002. GOB authorities have circulated the names of suspected terrorists and terrorist organizations listed on the United Nations (UN) 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224 to all financial institutions in Belize. There are no indications that charitable or nonprofit entities in Belize have acted as conduits for the financing of terrorist activities. Consequently, the government has not taken any measures to prevent the misuse of charitable and nonprofit entities from aiding in the financing of terrorist activities.

Belize has signed and ratified a Mutual Legal Assistance Treaty with the United States, which provides for mutual legal assistance in criminal matters and entered into force in 2003. Amendments to the MLPA preclude the necessity of a Mutual Legal Assistance Treaty for exchanging information or providing judicial and legal assistance to authorities of other jurisdictions in matters pertaining to money laundering and other financial crimes. Belize is a party to the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the 1988 UN Drug Convention. Belize is not a party to the UN Convention against Corruption. Belize is a member of the Organization of American States and the Caribbean Financial Action Task Force, a FATF-style regional body. The FIU became a member of the Egmont Group of financial intelligence units in 2004. However, Belize has not established a history of providing formal mutual assistance, and in fact has been a particularly nonreactive partner in the area of freezing and confiscating assets.

The Government of Belize should ensure effective implementation of its anti-money laundering and counterterrorist financing regime. The GOB should consider applying civil penalties as well as criminal penalties to further deter these financial crimes. The GOB should increase resources to provide adequate staffing levels and training to those entities responsible for enforcing Belize's anti-money laundering and counterterrorist financing laws, including the financial intelligence unit and the asset forfeiture regime. Belize should take steps to address the vulnerabilities in its supervision of its onshore and offshore sectors, particularly the lack of supervision of the gaming sector, including Internet gaming facilities, and ensure charitable and nonprofit entities cannot be used to aid in the financing of terrorism. Belize should immobilize bearer shares and ensure that the offshore sector complies with anti-money laundering and counterterrorist financing reporting requirements. The GOB should also become a party to the UN Convention against Corruption.

Bolivia

Bolivia is not a regional financial center; however, its money laundering activities continue to take place throughout the country, and are related primarily to the government's lack of political to combat money laundering, narcotics trafficking, public corruption, smuggling and trafficking of persons, as well as Bolivia's long tradition of bank secrecy and the lack of effective government oversight of nonbank financial activities facilitate the laundering of organized crime and narcotics trafficking profits, the evasion of taxes, and the laundering of other illegally obtained earnings. The majority of existing money laundering criminal investigations is located in the Department of Santa Cruz and associated with significant narcotics trafficking organizations operating from that area.

Bolivia's financial sector consists of 13 commercial banks, six private financial funds, nine mutual funds, 23 savings and credit cooperatives, 14 insurance companies, and one stock exchange, all of which are subject to the same anti-money laundering controls. The Bolivian financial system is highly dollarized, with approximately 90 percent of deposits and loans distributed in U.S. dollars rather than bolivianos, the local currency. Free trade zones exist in the cities of EI Alto, Cochabamba, Santa Cruz, Oruro, Puerto Aguirre and Desaguadero.

Most entities that move money in Bolivia continue to be unregulated. Hotels, currency exchange houses, illicit casinos, cash transporters, and wire transfer businesses are known to transfer money freely into and out of Bolivia without being subject to anti-money laundering controls. Informal exchange businesses, particularly in the Department of Santa Cruz, also transmit money in order to avoid law enforcement scrutiny. The Government of Bolivia (GOB) recognizes shortcomings in Bolivian financial regulation and proposals have been made to address these deficiencies through modifications to the existing legislation.

Bolivia's current anti-money laundering regime is based on Article 185 of Law 1768 of 1997. Law 1768 modifies the penal code and criminalizes money laundering related only to narcotics trafficking offenses, organized criminal activities and public corruption. It provides for a penalty of one to six years for money laundering and defines the application of asset seizure beyond drug related offenses. Article 185, however, cannot be applied unless the prosecution demonstrates in court that the accused participated in and was convicted of the predicated crime. Although terrorist acts are criminalized under the Bolivian Penal Code, the GOB lacks actual statutes that specifically criminalize the financing of terrorism or that grant the GOB authority to identify, seize, or freeze terrorist assets. Legislation that has been in draft for several years, and now currently in Congress, seeks to address this omission by amending the penal code to including the criminalization of terrorist financing.

Article 185 of Law 1768 created Bolivia's financial intelligence unit, the Unidad de Investigaciones Financieras (UIF), located within the Office of the Superintendence of Banks and Financial Institutions. The UIF's function is to conduct financial investigations in an effort to produce findings and evidence of money laundering activities and other financial crimes and to share this information with both the Bolivian National Police and the Public Ministry, as appropriate. The UIF is also responsible for implementing anti-money laundering controls, and may request that the Superintendent of Banks sanction obligated institutions for noncompliance with reporting requirements. After conducting an initial analysis, the UIF reports detected criminal activity to the GOB's Public Prosecutor. The UIF also performs on-site investigations of obligated entities to review their compliance with the reporting of suspicious transactions and can request additional information from obligated financial institutions to assist prosecutors with their investigations. Given the UIF's limited resources relative to the size of Bolivia's financial sector, compliance with reporting requirements is extremely low. The actual exchange of information and financial intelligence between the UIF and appropriate police investigative entities is also limited or, in some cases, non-existent.

Bolivia's UIF has endured substantial turmoil since 2006, when the GOB issued Supreme Decree 28695 proposing the replacement of Bolivia's UIF with a new "Financial and Property Intelligence

Unit" focused on combating corruption rather than money laundering. As a result of the decree, the UIF lost a significant amount of its staff and although the new Financial and Property Intelligence Unit was never implemented, Bolivia's UIF has been unable to recover. As of 2007, the UIF maintained a staff of seven; however, the lack of personnel, combined with inadequate resources and weaknesses in Bolivia's basic legal and regulatory framework fundamentally limits its reach and effectiveness as a financial intelligence unit (FIU).

Further complicating the situation for Bolivia's UIF is its relationship with the Egmont Group, an international network of FIUs that facilitates the exchange of financial intelligence and analysis. The Egmont Group amended its membership requirements in June 2004, requiring all member states to criminalize the financing of terrorism and their FIUs to receive STRs related to terrorist financing. In July of 2007, as a direct result of a lack of terrorism financing legislation within the existing Bolivian laws, the UIF received a "Letter of Suspension" from the Egmont Group for "noncompliance with the international mandate to have appropriate legislation addressing this issue." The GOB's continued lack of terrorist financing legislation since the Egmont Group's 2004 requirement went into effect resulted in Bolivia's expulsion from the Egmont Group of financial intelligence units in December 2008—an unprecedented move by the Egmont Group. The suspension bars the UIF from participating in Egmont meetings or using the Egmont Secure Web (the primary means of information exchange among Egmont members) to share information with other FIUs. To regain Egmont membership, Bolivia must reapply and provide written evidence of the UIF's compliance with Egmont requirements. The Egmont Group has offered, and continues to offer, assistance to the Bolivian FIU to address its structure and implementing laws to facilitate its re-admission to the Group.

The GOB's pro-coca policies have enabled drug trafficking organizations to become well entrenched in the country and another major blow to Bolivia's anti-money laundering regime is the expulsion of U.S. Drug Enforcement Administration (DEA) agents from the country in November 2008. This action is likely to diminish the effectiveness of several financial investigative groups operating in the country, including Bolivia's Financial Investigative Team (EIF), the Bolivian Special Counternarcotics Police (FELCN), and the Bolivian Special Operations Force (FOE).

The EIF was created in 2002 within Bolivia's FELCN and is responsible for investigating narcotics-related money laundering cases. Currently, there are three EIF units in Bolivia (La Paz, Santa Cruz, and Cochabamba) consisting of a total of 30 personnel (one civilian auditor, and 29 BNP/FELCN investigators). The National Director of the FOE seeks to expand these financial investigative units from 30 personnel nationwide to a total of 60, which would include four financial auditors, one national legal advisor, one national information technology specialist and 51 financial investigators. This initiative was still pending as of late 2008. During the last 12 months, the EIF reported six new money-laundering cases and a total of approximately $10 million in assets seized. The EIF, UIF, Public Ministry, National Police and FELCN have established mechanisms for the exchange and coordination of information, including formal exchange of bank secrecy information.

Under Supreme Decree 24771, obligated entities such as banks, insurance companies and securities brokers are required to identify their customers, retain records of every transactions for a minimum of ten years, and report to the UIF all transactions that are considered unusual (without apparent economic justification or licit purpose) or suspicious (customer refuses to provide information or the explanation and/or documents presented are clearly inconsistent or incorrect). Bolivia, until recently, had no requirement for these obligated entities to report cash transactions above a designated threshold, and no requirement stating that persons over a designated threshold.

On August 20, 2008, the GOB signed into law Supreme Decree 29681 requiring nationals and foreigners entering or leaving the country to declare the transportation of currency and also obligates any person or business with the intention of transporting, either into or out of the country, any amount of currency in excess of $50,000 to register the transaction with Bolivia's Central Bank. Additionally,

the decree states all transactions reported to customs in excess of $10,000 must be reported on a monthly basis to the UIF. Also, the GOB's Superintendent of Banks issues written instructions to the national banks directing them to report any cash transactions in excess of $10,000 or other suspicious financial activities to the UIF.

Corruption remains a serious issue in Bolivia. In the past, allegations against high-ranking law enforcement officials were routinely dismissed without further investigation. While some improvement in the effectiveness of investigations is apparent, few cases are fully prosecuted. On April 26, 2006, for example, the GOB promulgated Supreme Decree 28695, the Organizational Structure for the Fight against Corruption and Illicit Enrichment, as a means to further combat corruption in the police force and other government agencies. As of October 2008, the Bolivian National Police's Office of Professional Responsibility (OPR) investigated a total of 2,043 cases in 2008 involving allegations of misconduct and/or impropriety by police officers. Of these, 176 cases involved police officers assigned to Bolivia's Special Counter-Narcotics Force (FELCN); none resulted in findings of corruption. A total of 876 cases have been adjudicated before the Police Disciplinary tribunal, the remainder are still in the investigative stage and/or awaiting tribunal action.

There continue to be serious deficiencies in Bolivia's legal framework with regard to civil responsibility in financial and money laundering cases. Under Bolivian law, there is no protection for judges, prosecutors or police investigators who make good-faith errors while carrying out their duties. If a case is lost initially or on appeal, or if a judge rules that the charges against the accused are unfounded, the accused can request compensation for damages, and the judges, prosecutors or investigators can be subject to criminal charges for misinterpreting the law. This is particularly problematic for money laundering investigations since the legislation is full of inconsistencies and contradictions, and is open to wide interpretation. As a result, prosecutors are often reluctant to pursue money laundering investigations.

While traditional asset seizure continues to be employed by counternarcotics authorities, the ultimate forfeiture of assets continues to be problematic. The Directorate General for Seized Assets (DIRCABI) is responsible for confiscating, maintaining, and disposing of the property of persons either accused or convicted of violating Bolivia's narcotics laws. DIRCABI, however, has been poorly managed and plagued by corruption for years, and has only auctioned confiscated goods sporadically. In late 2006, then newly appointed DIRCABI staff, including the National Director and several Regional Directors, began initiating positive steps to improve the organization's internal operating procedures. In 2007, DIRCABI proposed Supreme Decree 29305, which was signed by the Bolivian President in October 2007 and provides for some positive changes relating to asset seizure, forfeiture, and sharing. DIRCABI is involved in drafting new civil asset forfeiture legislation to address persisting problems in terms of forfeited asset sharing among law enforcement entities. To address the inadequate management and related administrative issues that have plagued DIRCABI for years, special administrative legislation was submitted for approval that will resolve long standing organizational issues that resulted in questionable administrative procedures in these forfeiture cases. As of October 31, 2008, DIRCABI has initiated 615 asset forfeiture cases. In these 615 cases, 1,201 items were seized—the majority of which included electronic equipment, such as cellular phones. In addition, a total of 26 residences, 211 vehicles, as well as cash, jewelry, and other miscellaneous items were seized.

Bolivia is a party to the 1988 UN Drug Convention, UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Corruption, and the UN Convention against Transnational Organized Crime. Bolivia does not have a mutual legal assistance agreement with the United States, but is a party to the Inter-American Convention on Mutual Assistance in Criminal Matters. Bolivia is also a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group on Money Laundering.

The GOB is currently a sanctioned member of the Financial Action Task Force for South America (GAFISUD). The GAFISUD placed sanctions on Bolivia in July 2007 as a result of the GOB's failure to pay three years of its membership dues. The GOB was able to make partial payment of its arrears and a bill is currently pending in Bolivia's Congress to authorize payment of its remaining debt to GAFISUD. At the GAFISUD December 2008 plenary meeting, GAFISUD members agreed to continue sanctions that prohibit Bolivia from having a voice or vote at GAFISUD plenary meetings, with the expectation that Bolivia will have met the requirements to fully reinstate its membership by the June 2009 plenary meeting.

Several of Bolivia's current AML/CTF regime deficiencies can be remedied if the GOB were to enact current draft legislation to improve Bolivian law in the area of financial investigations. With support from the USG and others, the GOB has formed a working group composed of key GOB ministry and police representatives with the goal of creating new legislation to address issues such as the interception of communications, money laundering, civil forfeiture, modifications to the existing Criminal Code of Procedures, consensual recordings, and cooperation agreements. In addition, within this legislative initiative, the area of terrorism financing would be addressed along with a new special administrative law to improve the functions of DIRCABI. The GOB completed this draft legislation in October 2008, received interagency approval, and submitted the bill to the Bolivian Congress for review in late 2008. It is anticipated that the legislation will be approved and written into law at the beginning of 2009. This legislation would significantly improve the abilities of the GOB investigators and prosecutors to more successfully attack criminals and organizations involved in illicit financial activities in Bolivia, including terrorism financing.

The GOB should take all necessary steps to ensure that the draft anti-money laundering legislation is enacted and conforms to international standards. Among the most important legislative adjustments, it is imperative that the GOB criminalizes terrorist financing and allow for the blocking of terrorist assets; doing so is not only mandated by Bolivia's commitments as a member of the United Nations and GAFISUD, but could improve the likelihood that the UIF may successfully re-apply for Egmont Group membership. In addition, money laundering should be an autonomous offense without requiring prosecution for the underlying predicate offense, and currently unregulated sectors, particularly designated nonfinancial businesses and persons, should be subject to anti-money laundering and counterterrorist financing controls. Bolivia should also ensure that the UIF has sufficient staff and resources. The GOB should also pay the remainder of its GAFISUD dues to avoid being fully suspended from GAFISUD.

Bosnia and Herzegovina

Bosnia and Herzegovina (BiH) has a cash-based economy and is not an international, regional, or offshore financial center. The laundering of illicit proceeds derives from criminal activity including the proceeds from smuggling, corruption, and widespread tax evasion. Due to its porous borders and weak enforcement capabilities, BiH is a significant market and transit point for illegal commodities including cigarettes, narcotics, firearms, counterfeit goods, lumber, and fuel oils. BiH authorities have had some success over the past few years in clamping down on money laundering through the formal banking system. Statistics from Bosnia's financial intelligence unit (FIU) indicate that financial crimes have increased over the past year. Bosnia is also vulnerable to terrorist financing. The cash-based economy and weak border controls on bulk cash couriers contribute to BiH as an attractive venue for terrorist financiers and organized criminal elements to carry out illicit financial activities.

Corruption is also a serious problem in BiH. The European Commission's November 2008 Progress Report for Bosnia identified widespread corruption as one of the key problems in the country. In addition, Transparency International has recently ranked Bosnia as the most corrupt country in the Balkan region, stating that corruption is of particular concern in Bosnia because it involves political

corruption as well as corruption in privatization and public procurement procedures. Bosnia adopted an anticorruption strategy in 2006, but has since failed to fully implement any aspects of the plan.

It is likely that trade-based money laundering occurs in BiH, but there is no indication that law enforcement has taken any action to combat it. There are five active Free Trade Zones in BiH, with production based mainly on automobiles and textiles. There have been no reports that these trade zones are used in trade-based money laundering. The Ministry of Foreign Trade and Economic Relations is responsible for due diligence and monitors the activities of these zones.

The threat posed by bulk cash couriers is not well understood in BiH. Remittances from abroad are estimated to be in the millions of U.S. dollars annually, and constitute as much as 20 percent of the BiH gross domestic product. Many of these remittances likely enter the country in the form of cash. Customs officials are required to report any cross-border transportation of cash in excess of KM 10,000 (approximately $6,770), but this regulation is not enforced and there is no declaration or disclosure system in place for cash entering the country.

The September 2006, International Monetary Fund's Financial System Stability Assessment report praises Bosnia and Herzegovina for the progress made since the 2005 mutual evaluation by the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), a Financial Action Task Force-style regional body. However, the report also cites problems with information-sharing, coordination, and communication, as well as jurisdictional issues between the Financial Police and other State agencies. Those problems continue to exist with little evident correction.

The capabilities of the BiH anti-money laundering/counterterrorist financing (AML/CTF) regime should be viewed in the context of Bosnia's decentralized political structure. There are multiple jurisdictional levels in Bosnia and Herzegovina, including the State, the two entities (the Federation of Bosnia and Herzegovina (the Federation) and the Republika Srpska (the RS)), and Brcko District. The Federation is further divided into ten cantons. Criminal and criminal procedure codes from the State, the two entities, and Brcko District were enacted and harmonized in 2003. Each jurisdiction, however, maintains its own separate supervision and enforcement bodies. Although State-level institutions are becoming more firmly grounded and are gaining increased authority, there remains a fair amount of confusion regarding jurisdictional matters between the entities and State-level institutions. This confusion undermines State-level institutions and impedes efforts to improve operational capabilities to combat money laundering and terrorist financing. Unless otherwise specified, relevant laws and institutions are at the State level.

Money laundering is a criminal offense in all state and entity criminal and criminal procedure codes. At the State level, the Law on the Prevention of Money Laundering, enacted in 2004, takes an "all serious crimes" approach and determines the measures and responsibilities for detecting, preventing, and investigating money laundering and terrorist financing. The law also prescribes measures and responsibilities for international cooperation and establishes an FIU within the State Investigative and Protection Agency (SIPA). Those convicted of money laundering exceeding the equivalent of $30,000 receive prison terms of between one and ten years. For lesser amounts, the penalty is imprisonment between six months and five years.

The Law on the Prevention of Money Laundering requires 26 types of entities to report to the FIU all transactions of $18,000 or more as well as all transactions (regardless of amount) suspected of connections to money laundering or terrorist financing. The money laundering law applies to all banks, individuals and several nonbank financial institutions (NFIs) and designated nonfinancial businesses and professions (DNFBPs), including post offices, investment and mutual pension companies, stock exchanges and stock exchange agencies, insurance companies, casinos, currency exchange offices and intermediaries such as lawyers and accountants. In practice, most NFIs and DNFBPs do not understand the law, thereby resulting in very low reporting from those sectors. The

FIU is developing an automated AML reporting system, on which all bodies responsible for reporting will eventually be trained. In addition to cash and suspicious transaction reporting requirements, the law requires that customs officials from the Indirect Tax Authority (ITA) forward to the FIU all reports of cross-border transportation of cash and securities in excess of $6,000. All banks have the ability to send electronic cash transaction reports (CTRs) and suspicious transactions reports (STRs) to the FIU, which then stores them in a central database. The banking sector and the ITA file the majority of reports.

BiH has not enacted bank secrecy laws that prevent the disclosure of client and ownership information to bank supervisors and law enforcement authorities. The law requires banks and other financial institutions to know, record, and report the identity of customers engaging in significant transactions, including currency transactions above the equivalent of $18,000. Financial institutions must maintain records for 12 years to respond to law enforcement requests. Bosnian law protects reporting individuals with respect to law enforcement cooperation.

Although there is no State-level banking supervision agency, entity level banking supervision agencies oversee and examine financial institutions for compliance AML/CTF laws and regulations. There is, however, no formal supervision mechanism in place for nonbank financial institutions and intermediaries. Nonbank financial transfers are reportedly very difficult for law enforcement and customs officials to investigate. This is due not only to a lack of reporting, but also to a lack of understanding of indigenous methodologies and alternative remittance systems, many of which are found in the underground economy and are enabled by smuggling and the misuse of trade.

Police at both the State and entity levels investigate financial crimes. At the State level, SIPA and the FIU are responsible for investigating financial crimes. In addition to an Economic Crime Unit, the Federation Police has a specialized Financial Police Unit that focuses on public corruption, economic crimes, money laundering, and cybercrime. The RS police has a Special Investigations Unit to investigate financial crimes. Both the Federation Police and the RS police lack adequate resources and training. In addition, both agencies acknowledge that the level of cooperation and information exchange with SIPA is poor and needs improvement.

The ITA suffers from a lack of resources and sufficiently trained personnel. Because BiH is largely a cash economy, it is typical for individuals to carry large amounts of cash, even across borders. Bosnia and Herzegovina also receives a significant volume of remittances from emigrants. Official remittances constitute over 17 percent of GDP. While some of these will enter the country through bank transfers, others cross the border via courier.

The Financial Intelligence Department (FID), Bosnia-Herzegovina's FIU, is a hybrid body, performing analytical duties while maintaining limited criminal investigative responsibilities. The FID receives, collects, records, analyzes, and forwards information related to money laundering and terrorist financing to the State Prosecutor. It also provides expert support to the Prosecutor regarding financial activities and handles international cooperation on money laundering issues. Officially, the FID has access to the records of other government entities; and formal mechanisms for interagency information sharing are in place. In practice, however, cooperation between the FID and other government agencies is weak, with little information shared among agencies. This applies particularly to information sharing between the FID and the different police forces. However, banking agencies do share information with the FID. When suspicion of illicit activity exists, the FID has the power to freeze accounts for five days. During this time, if the FID is able to collect sufficient evidence of possible criminal activity, it may forward the case to the Prosecutor. At that point, the freeze on the accounts may be extended. During the first nine months of 2008, the FID reports it froze assets in only one case, in the amount of KM 4.3 million ($2,900,000).

The FID currently faces several challenges. Information sharing and interagency cooperation are major operational deficiencies of the FID. Although it receives and analyzes information from reporting

entities, it does not effectively share the results of its analysis with relevant law enforcement agencies. One reason for this is an ambiguous provision in the AML law that does not clearly define the FID's obligation to disseminate information to appropriate law enforcement entities. FID officials have interpreted the information sharing provision in the AML law so narrowly that it has resulted in a virtual standstill in the dissemination of reports to agencies outside of SIPA. The failure by the FID to properly disseminate its information has greatly isolated the agency, affecting not only communication and cooperation between the FIU and law enforcement but the overall effectiveness of the FID as well.

Management of the data submitted to the FID is another problem facing the FIU. Obligated entities submit reports to the FIU through an electronic reporting system. However, prior to the implementation of the electronic reporting system, institutions submitted hardcopy reports which were then entered manually into the FID's database. There is currently a backlog of approximately 140,000 reports that have not yet been input into the FID's database.

In the first nine months of 2008, the FID received 208,378 CTRs from banks and other financial institutions. Of these, the FID identified 47 cases as suspicious and investigated them. Of these 47 cases, the FID submitted seven reports to the BiH Prosecutor. Since BiH established its AML regime in 2004, the Court of BiH has pronounced 38 money laundering verdicts: 17 legally binding verdicts in 2004 and 2005 (in which the total amount of laundered money was nearly $10,900,000, and for which nearly $800,000 in assets was forfeited), 12 first instance verdicts in 2006, and nine first instance verdicts in 2007. Statistics for 2008 are not yet available. A major problem facing BiH is the high rate of verdicts overturned or modified on appeal (which is not exclusively a problem for money laundering convictions). So it is possible that some of the 2006 and 2007 verdicts may yet be overturned. The FID is not the only active agency in the AML regime: the RS entity police agency and the Federation Financial Police, among others, all reported money laundering-related cases. In 2008, the Bosnian Court system pronounced five money laundering verdicts involving a total of seven people. Out of these five cases, four included prison sentences and one a suspended sentence.

BiH has no specific asset forfeiture law as regards money laundering, with the exception of the Persons Indicted for War Crimes (PIFWC) support laws that allow for the seizure of PIFWC assets or assets of those providing material support to them. Articles 110 and 111 of the BiH Criminal Code (along with similar laws in the harmonized entity and Brcko Criminal Codes) are the only legal provisions that authorize asset forfeiture. These provisions authorize the "confiscation of material gain" (or a sum of money equivalent to the material gain if confiscation is not feasible) from illegal activity. The law does not provide for the seizure and forfeiture of assets that may have been used in or facilitated the commission of the illegal activity. The courts administer confiscation, which can only take place as part of a verdict in a criminal case. The courts decide whether the articles will be "sold under the provisions applicable to judicial enforcement procedure, turned over to the criminology museum or some other institution, or destroyed. The proceeds obtained from sale of such articles shall be credited to the budget of Bosnia and Herzegovina." Courts do not have the administrative mechanisms in place to seize assets, maintain them in storage, dispose of them, or route the proceeds to the appropriate authorities. Article 133 of the criminal code also allows the courts to seize property as punishment for criminal offenses for which a term of imprisonment of five years or more is prescribed. In such cases, asset seizure is possible without proving a specific relationship between the assets and the crime. There is no mechanism for civil forfeiture, although, Article 110 (3) of the Criminal Code appears to contemplate a civil or quasi-civil forfeiture: "a separate proceeding if there is probable cause to believe that the gain derives from a criminal offense and the owner is not to give evidence that the gain was legally acquired." There are no laws for sharing seized assets with other governments. BiH authorities have the authority to identify, freeze, seize, and forfeit terrorist-finance-related and other assets. The banking agencies (Federation and RS Banking Agencies) in particular have the capability to freeze assets without undue delay. The banking community cooperates with law enforcement efforts to trace funds and freeze accounts.

Article 202 of the Criminal Code criminalizes terrorist financing. Entity banking agencies are cognizant of the requirements to sanction individuals and entities listed by the UNSCR 1267 Sanctions Committee's consolidated list, but the State authorities do not regularly circulate this list to entity authorities. The U.S. Embassy, however, provides updates to appropriate entity authorities. There is no one government entity that regulates or supervises the nongovernmental organization (NGO) sector, but NGOs are subject to some supervision from the relevant ministry, tax administration, labor or other inspectors.

In 2004, the government disrupted the operations of Al Furqan (aka Sirat, Istikamet), Al Haramain & Al Masjed Al Aqsa Charity Foundation, and Taibah International, organizations listed by the UNSCR 1267 Committee as having direct links with al-Qaida. Authorities continue to investigate other organizations and individuals for links to terrorist financing. In 2006, after a cooperative investigation between BiH and law enforcement authorities in several European Union countries, authorities initiated a prosecution at the Court of Bosnia and Herzegovina against five people suspected of terrorist crimes. Four of the defendants were found guilty in January 2007, and this verdict was affirmed by a three-judge appellate panel of the BiH State Court in June, making the verdict final and binding. In March 2008, five Bosnian Muslims belonging to a radical group were arrested for suspected terrorist activity and handed over to the State Prosecutor's Office for investigation. Weapons, including mines and other explosive devices, as well as materials for making explosive devices, were found and seized during the operation. They were subsequently released by the prosecutor for lack of admissible evidence pertaining to formal terrorism charges. A Bosnian investigation is still ongoing.

Bosnia and Herzegovina has no Mutual Legal Assistance Treaty with the U.S. BiH succeeded to the extradition treaty concluded between the Kingdom of Serbia and the United States in 1902; while this treaty covers some financial crimes, it does not address contemporary forms of money laundering. There is no formal bilateral agreement between the United States and BiH regarding the exchange of records in connection with narcotics investigations and proceedings, however, authorities have made good faith efforts to exchange information informally with officials from the United States. BiH is a party to the 1988 UN Drug Convention (by way of succession from the former Yugoslavia), the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the UN Convention for the Suppression of the Financing of Terrorism. Unfortunately, on many occasions, BiH has not passed implementing legislation for the international conventions to which it is a party. Bosnia is a member of MONEYVAL and the FID is a member of the Egmont Group. Bosnia is scheduled to undergo a mutual evaluation by MONEYVAL in 2009.

The Government of Bosnia and Herzegovina (GOBiH) should continue to strengthen institutions with responsibilities for money laundering prevention, particularly those at the State level. Due to a lack of resources and bureaucratic politics, SIPA and the FID, like many State institutions, remain under-funded and under-resourced. The GOBiH should make efforts to increase funding for its AML/CTF programs and enhance cooperation between concerned departments and agencies. With regard to the FID, BiH should amend its AML law to clarify the FID's obligation to disseminate information outside of SIPA. The FID also needs to reduce the backlog of reports that have not been input into its database. Although prosecutors, financial investigators, and tax administrators have received training on tax evasion, money laundering, and other financial crimes, the GOBiH should enhance their capacity to understand diverse methodologies, and aggressively pursue investigations. BiH authorities should undertake efforts to understand the illicit markets and their role in trade-based money laundering and alternative remittance systems. The banking agencies in BiH should increase awareness by improving outreach programs to address major vulnerabilities, including the identification of shell companies and beneficial owners. In addition, GOBiH should implement formal supervisory mechanisms for nonbank financial institutions and intermediaries, and NGOs. BiH law enforcement and customs authorities should take additional steps to control the integrity of the borders

and limit smuggling. The GOBiH should study the formation of centralized regulatory and law enforcement authorities. BiH should take specific steps to completely implement its anticorruption strategy and to combat corruption at all levels of commerce and government. BiH also should adopt a comprehensive asset forfeiture law that provides a formal mechanism for the administration of seized assets, and should consider establishing a civil forfeiture regime. The government should enact implementing legislation for the international conventions to which it is a party.

Brazil

Brazil is the world's fifth largest country in size and population, and in 2008 its economy remains the tenth largest in the world. Brazil is considered a regional financial center for Latin America. It is also a major drug-transit country. Brazil maintains adequate banking regulations, some controls of capital flows, and requires disclosure of the ownership of corporations. Money laundering in Brazil is primarily related to domestic crime, especially drug-trafficking, corruption, organized crime, and trade in various types of contraband. Trade of all kinds generates funds that may be laundered through the banking system, real estate investment, financial asset markets, luxury goods or informal financial networks. An Inter-American Development Bank study of money laundering in the region found that Brazil's relatively strong institutions helped keep the incidence of money laundering to below average for the region.

Terrorist financing is not an autonomous offense in Brazil, although the money laundering bill currently awaiting legislative action contains language effecting that change. The bill would make it a crime to directly or indirectly provide or to receive from any person or group funds, goods, services or anything else of value, with the intention of causing public panic, and/or trying to constrain or influence a government or international body to act or refrain from acting. Those convicted would be punished for up to 12 years in prison. To implement fully this important change and other aspects of its financial crimes regime, Brazil intends to enact legislation that will provide for the effective use of advanced law enforcement techniques such as undercover operations, controlled delivery, and the use of electronic evidence and task force investigations that are critical to the successful investigation of complex crimes, such as money laundering. Currently, such techniques can be used only for information purposes, and are not admissible in court.

The U.S. Government (USG) continues to believe the Brazil-Paraguay-Argentina Tri-Border Area (TBA) to be a source of terrorist financing, although the Government of Brazil (GOB) maintains that it has not seen any such evidence. That said, there may be as much or more reason to be concerned about other areas of the country. GOB and local officials in the states of Mato Grosso do Sul and Parana, for example, have reported increased involvement by Rio de Janeiro and Sao Paulo gangs in the already significant trafficking in weapons and drugs that plagues the states in the tri-border area. Consequently, antismuggling and law enforcement efforts by state and federal agencies have increased. In addition to weapons and narcotics, a wide variety of counterfeit goods, including CDs, DVDs, and computer software (much of it of Asian origin), are routinely smuggled across the border from Paraguay into Brazil. Brazilian customs authorities have continued their efforts to combat contraband in the TBA given the resulting loss of tax revenues.

Brazil's anti-money laundering policy is to advance six goals: improve coordination between federal and state anti-money laundering agencies; develop and make maximum use of computerized databases and public registries to facilitate monitoring and enforcement; constantly evaluate and improve existing mechanisms; increase international cooperation in enforcement and the recovery of assets; promote an anti-money laundering culture in Brazil; and prevent violations before they occur through the foregoing.

Brazil's first anti-money laundering legislation passed in 1998 and has since been amended by subsequent legislation, decree and regulation. Law 9.613 criminalizes money laundering related to

drug trafficking, terrorism, arms trafficking, extortion by kidnapping, public administration, the national financial system and organized crime. The 1998 statute requires that individuals bringing more than 10,000 reais (then $10,000, now $4,700) in cash, checks, or traveler's checks into Brazil must fill out a customs declaration. Subsequent modification to the law and associated regulations criminalize the corruption or attempted corruption of foreign public officials involving international commercial transactions, and establishes terrorist financing as a predicate offense for money laundering. The current legal regime also establishes crimes against foreign governments as predicate offenses, and requires the Central Bank to create and maintain a registry of information on all bank account holders.

The 1998 anti-money laundering statute also created Brazil's financial intelligence unit, the Conselho de Controle de Atividades Financeiras (COAF), which is housed under the Ministry of Finance. COAF staff includes representatives from regulatory and law enforcement agencies, including the Central Bank and Federal Police, and is empowered to request financial information on any individual suspected of criminal activity from all government entities. COAF has a staff of 43 and expects to add 25 new personnel in 2009.

Entities under the authority of the Central Bank, the Securities Commission (CVM), the Private Insurance Superintendence (SUSEP), and the Office of Supplemental Pension Plans (PC), are required to file suspicious activity reports (SARs) with their respective regulator, which passes them to COAF. COAF directly regulates and receives SARs from those financial sectors not already under the jurisdiction of another supervising entity, such as commodities traders, real estate brokers, credit card companies, money remittance businesses, factoring companies, gaming and lottery operators, bingo parlors, dealers in jewelry and precious metals, and dealers in art and antiques.

The Central Bank's Department to Combat Exchange and Financial Crimes (DECIC) examines entities under the supervision of the bank to ensure compliance with suspicious transaction reporting requirements, and forwards information on the suspect and the nature of the transaction to COAF. In 2005, DECIC was able to bring on-line a national computerized registry of all current accounts in the country. A Central Bank regulation issued that same year requires banks to report identifying data on all parties to foreign exchange transactions and money remittances, regardless of the amount involved.

In addition to filing SARs, banks are also required to inform the Central Bank of institutional transactions exceeding 100,000 reais ($57,000) and "unusual" amounts transacted by individuals. Lottery operators must notify COAF of the names and identifying information of winners of three or more prizes equal to or higher than 10,000 reais within a 12-month period. Subsequent changes in the law authorize the monitoring of transactions with possible links to terrorism and by politically exposed persons.

SUSEP requires insurance companies and brokers to report large policy purchases, settlements or otherwise suspicious transactions to both SUSEP and COAF. Insurance-related activities by or on behalf of politically exposed persons are also monitored. In addition, on January 8, 2008, the Securities Commission (CVM) extended monitoring/reporting requirements to include dealers in luxury goods and persons or companies that engage in activities involving a high volume of cash transactions.

COAF has direct access to the Central Bank database, so that it can review its SARs and information about all current accounts. COAF also has access to government databases, and is authorized to request additional information directly from the entities it supervises and the supervisory bodies of other reporting entities. Complete bank transaction information may be provided to government authorities, including COAF, without a court order. Brazilian authorities that register with COAF may directly access COAF databases via a password-protected system.

During the first 10 months of 2008, COAF received information regarding 226,413 cash and 296,070 noncash transactions, an increase of 55 percent compared to 2007. During the same period, the Central Bank received 830,257 reports of transactions exceeding 100,000 reais and 367,566 reports were submitted to SUSEP regarding activities in the insurance sector. Through October 2008, COAF has provided 1,002 Financial Intelligence Reports involving 8,997 individuals to cooperating agencies. The Justice Ministry used COAF reports to seize 640 million reais in 2008. COAF has referred 17 cases for administrative sanctions this year, resulting in fines of 3.8 million reais.

Additional legislative changes are currently under consideration by the Brazilian legislature. The pending legislation, if approved in its current form, would facilitate greater law enforcement access to financial and banking records during investigations, criminalize illicit enrichment, allow seized assets to be monetized to preserve their value, and facilitate prosecution of money laundering cases by making it an autonomous offense. The proposed changes would also help to bring the Brazilian legal regime in line international anti-money laundering standards. This legislation is considered a priority, and is expected to be voted on by Congress shortly.

The National Corruption and Money Laundering Strategy Task Force (ENCCLA—Estratégia Nacional de Combate a Corrupção e Lavagem de Dinheiro) is comprised of GOB and state agencies with jurisdiction over money laundering and other financial crimes and began convening periodic strategy and planning sessions in 2003. Twenty-eight agencies, ranging from the National Intelligence Agency to the Brazilian Banking Federation attended the first meeting; 51 participated in 2007. In November 2008, ENCCLA met in Salvador, Bahia. Participants from federal, state, and municipal governments took part and established ways to confront administrative fraud, domestic money laundering through business activities, and to regulate investigation techniques.

Some of the agencies, and most of the laws and regulations that comprise Brazil's anti-money laundering apparatus were conceived within the ENCCLA framework, including pending revisions of the current statute. ENCCLA members have also drafted a bill imposing conditions on banking privacy and allowing for the forfeiture of assets. The National Registry of Account Holders, which permits authorities to monitor transactions between individuals and corporations utilizing the national financial system, was also an ENCCLA initiative. Prior to the creation of the registry, information requests from judges could take several weeks to process. Now, detailed information can be compiled and forwarded within 24 hours of the request.

ENCCLA also helped create the Justice Ministry's Department of Asset Recovery, which, among other duties, is responsible for international cooperation on money laundering cases and is empowered to share seized forfeited assets with other countries. The determination that "politically exposed" individuals merited special attention was first proposed at a 2006 ENCCLA meeting. The Central Bank now maintains a registry of 30,000 office holders, persons who have held office in the past five years, and persons who appear to have or have had some financial nexus to them.

The GOB reported regular increases in the number of money laundering investigations, trials and convictions beginning in 2003. The annual number of investigations grew from 198 in 2003 to 625 in the first three quarters of 2006. These investigations led to 26 trials to 41 in the first three quarters of 2006, while convictions increased from 172 in 2003 to 866 in 2006. One reason for the growing number of money laundering prosecutions is the number of cases that are resulting from the Banestado bank scandal of the late 1990s. Through 2008, this investigation has resulted in 95 indictments against 684 persons, of which 97 have already been tried and found guilty. Yet another reason for the increase in investigations since 2005 is the establishment of Brazil's Trade Transparency Unit (TTU) that identifies discrepancies in trade data that are indications of trade-based money laundering. In its first year of operation, Brazil's TTU (with the assistance of U.S. DHS ICE agents) uncovered a discrepancy so large that 250 search warrants were issued throughout Brazil and eventually led to 128 arrest warrants. The number of investigations and convictions since 2006 is still not available, as the

Ministry of Justice remains in the process of developing a unified reporting system that would account for information from the various money laundering courts involved.

The GOB also credits the creation of specialized money laundering court branches, founded in 2003, for the increasing number of successful prosecutions. Fifteen such courts have been established in fourteen states, including two in São Paulo, with each court headed by a judge who receives specialized training in national money laundering legislation. A 2006 national anti-money laundering strategy goal was formed aimed to build on the success of the specialized courts by creating complementary specialized federal police financial crimes units in the same jurisdictions. In 2008, the Federal Police established such units in the Federal District (Brasilia), and the states of Rio de Janeiro and São Paulo. All other 24 states have established financial working groups.

Brazil has established systems for identifying, tracing, freezing, seizing, and forfeiting narcotics related assets. The COAF and the Ministry of Justice manage these systems jointly. Police authorities and the customs and revenue services are responsible for tracing and seizing assets, and have adequate police powers and resources to perform such activities. A GOB computerized registry of all seized assets to improve tracking and disbursal is currently being tested and is now in the "pilot" phase. The judicial system has the authority to forfeit seized assets, and Brazilian law permits the sharing of forfeited assets with other countries.

The GOB has generally responded to U.S. efforts to identify and block terrorist-related funds. Since September 11, 2001, the COAF has run inquiries on hundreds of individuals and entities, and has searched its financial records for entities and individuals on the UNSCR Sanctions Committee's consolidated list. None of the individuals and entities on the consolidated list has been found to be operating or executing financial transactions in Brazil, and the GOB insists there is no evidence of terrorist financing in Brazil.

The USG has placed nine individuals and two entities in the TBA on its list of Specially Designated Nationals, because they have provided financial and/or logistical support to Hezbollah. The nine individuals operate in the TBA and all have provided financial support and other services for Specially Designated Global Terrorist Assad Ahmad Barakat, who was previously designated by the U.S. Treasury in June 2004 for his support to Hezbollah leadership. The two entities, Galeria Pag and Casa Hamze, are located in Ciudad del Este, Paraguay, and have been used to generate or move terrorist funds. The GOB has publicly disagreed with the designations, stating that the United States has not provided any new information that would prove terrorist financing activity is occurring in the TBA.

Brazil is party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the UN Convention for the Suppression of the Financing of Terrorism. Brazil is a member of the Financial Action Task Force (FATF) and assumed its presidency for one year in July 2008. Brazil was a founding member of the Financial Action Task Force against Money Laundering in South America (GAFISUD), and held the GAFISUD presidency in 2006. Brazil is also a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Brazil's financial intelligence unit, the Council for the Control of Financial Activities (COAF), has been a member of the Egmont Group of financial intelligence units since 1999.

The Mutual Legal Assistance Treaty between Brazil and the United States entered into force in 2001, and a bilateral Customs Mutual Assistance Agreement, signed in 2002, became effective in 2005. Using the Customs Agreement framework, the GOB and U.S. Immigration and Customs Enforcement in 2006 established a Trade Transparency Unit (TTU) in Brazil to detect money laundering via trade transactions. The GOB also participates in the "3 Plus 1" Security Group (formerly the Counter-Terrorism Dialogue).

The Government of Brazil should criminalize terrorist financing as an autonomous offense. In order to successfully combat money laundering and other financial crimes, Brazil should ensure the passage of legislation to regulate the sectors in which money laundering is an emerging issue. Brazil should enact and implement legislation to provide for the effective use of advanced law enforcement techniques in order to provide its investigators and prosecutors with more advanced tools to tackle sophisticated organizations that engage in money laundering, financial crimes, and terrorist financing. Brazil should also enforce currency controls and cross-border reporting requirements, particularly in the TBA and among designated nonbanking financial businesses and professions. Additionally, COAF must continue to fight against corruption and ensure the enforcement of existing anti-money laundering laws, including the obligation for all financial institutions to report transactions suspected of being related to terrorist financing.

British Virgin Islands

The British Virgin Islands (BVI) is a Caribbean overseas territory of the United Kingdom (UK), and remains vulnerable to money laundering due to drug trafficking and the exploitation of its offshore financial services.

The BVI is considered a major offshore financial center with the industry contributing nearly fifty percent of the Government's annual revenue. As of June 2008, the BVI has approximately nine banks, nine money remitters, 2,840 active mutual funds, 31 local insurance companies, 392 captive insurance companies, 213 trust licenses, eight authorized custodians, 22 company management companies, 117 registered agents, 532 limited partnerships, 10,666 local companies, and 445,865 active BVI business companies or international business companies (IBCs).

The International Business Companies Act (IBCA) of 1984 was created to facilitate companies wishing to conduct international transactions from a tax exempt environment. According to the IBCA, IBCs registered in the BVI cannot engage in business with BVI residents, provide registered offices or agent facilities for BVI incorporated companies, or own an interest in real property located in the BVI (except for office leases). All IBCs must be registered in the BVI by a registered agent; and the IBC or the registered agent must maintain an office in the BVI. The process for registering banks, trust companies, and insurers is governed by legislation that requires detailed documentation, such as a business plan and vetting by the appropriate supervisor within the Financial Services Commission (FSC). Registered agents must verify the identities of their clients.

As a UK overseas territory, the Government of the British Virgin Islands (GOBVI) has to comply with the European Union Code of Conduct on Business Taxation. The code, among other things, requires that local and offshore companies be treated equally for tax purposes. To address this, and to update the BVI companies' legislation, the BVI Business Companies Act (BCA) 2004 came into force in 2005. The BCA superseded the IBCA act in January 2007, and now exclusively regulates all companies incorporated in the BVI. The BCA retains many of the same requirements of the IBCA including exemption from BVI taxes, privacy of directors and share registries, no director member residency requirements, and no requirement to file accounts or retain visible and tangible evidence of incorporation. The BCA places all companies, offshore and onshore, within a zero tax regime. Under the BCA, a company limited by shares may issue bearer shares that are immobilized or registered through an authorized custodian. IBCs registered before 2005 with bearer shares have until 2009 to register their bearer shares with an authorized custodian.

Companies registered under the IBCA were provided a two-year transition period. During this period, IBCs had the option of re-registering as business companies under the BCA. Any IBC that did not re-register was automatically re-registered as a business company on January 1, 2007. While the IBCA only permitted the incorporation of companies limited by shares, the BCA offers seven different types of companies: companies limited by shares (the most widely used vehicle); companies limited by

guarantee authorized to issue shares (typically used for structuring transactions by combining equity and guarantee membership); companies limited by guarantee (not authorized to issue shares); unlimited companies (authorized to issue shares); unlimited companies (not authorized to issue shares); restricted purposes companies (used primarily in structured finance and securitization transactions); and segregated portfolio companies (presently limited to insurance companies and mutual funds). The BCA permits the use of numbered names for businesses, i.e. BVI Company # (followed by a number). If a company chooses this format, it will also be permitted to have a foreign character name; an English translation of the name is not required. The GOBVI reports that Asian countries continue to be a high user of BVI companies, and predicts that the use of BVI companies by Asian countries will increase in the future.

The Financial Services Commission (FSC) is the independent regulatory authority responsible for the licensing and supervision of regulated entities, which includes banking and fiduciary businesses, investment businesses, insolvency services, accountants, insurance companies, and company management and registration businesses. The FSC is also responsible for off-site and on-site inspections of these institutions. The Financial Services (Administrative Penalties) Regulations went into effect in January 2007, and are intended to deter and penalize regulated entities that are found to be noncompliant with BVI regulatory laws. The lowest penalty that may be imposed is $100 and the highest is $20,000. From January to June 2008, the FSC conducted eight on-site inspections and issued four warnings, one advisory, and assessed one fine.

The FSC cooperates with foreign counterparts and law enforcement agencies. In 2000, the Information Assistance (Financial Services) Act (IAFSA) was enacted to increase the scope of cooperation between the BVI's regulators and regulators from other countries. In 2007, the FSC published the Handbook on International Cooperation and Information Exchange. The handbook is publicly available via the FSC's website and explains the statutory mandates and regulations established in the BVI to facilitate and improve international cooperation.

The Proceeds of Criminal Conduct Act 1997 (POCCA) criminalizes money laundering in the BVI. The POCCA establishes all indictable offenses except drug trafficking as predicates for money laundering; drug trafficking predicated money laundering is established under similar provisions in the Drug Trafficking Offenses Act 1992 (DTOA). The POCCA outlines penalties for money laundering. Upon summary conviction, penalties include six months imprisonment or a fine not exceeding three thousand dollars or both; and on indictment to a term of imprisonment not exceeding 14 years or a fine of $20,000 dollars or both. The POCCA and the DTOA allows the BVI Court to grant confiscation orders against those convicted of an offense or who have benefited from criminal conduct. Although procedures exist for the freezing and confiscation of assets linked to criminal activity, including money laundering and terrorist financing, the procedures for the forfeiture of assets not directly linked to narcotics related crimes are unclear.

In February 2008, The Anti-Money Laundering Regulations (AMLR) replaced the Anti-Money Laundering Code of Practice 1999, and the Anti-Money Laundering and Terrorist Financing Code of Practice 2008 (AMLTFCOP) revoked The Guidance Notes 1999. The AMLTFCOP establishes a risk based approach to anti-money laundering (AML) and counterterrorist financing (CTF) supervision and compliance. Issued by the FSC, the AMLTFCOP applies to all financial institutions and designated nonfinancial businesses and professions (DNFBPs) including charities and nonprofit associations. Car dealers, yacht dealers, dealers in precious metals and stones, dealers in heavy machinery, and leasing companies were brought under the sphere of the BVI's AML regime through the Nonfinancial Business (Designation) Notice in February 2008. The Financial and Money Services Act 2008 (FMSA) will require entities that engage in money and currency exchange, money or value transfers, financial services businesses to become regulated entities and subject to the AMLR and the AMLTFCOP.

The AMLTFCOP identifies procedures for customer due diligence, identifying beneficial owners and politically exposed persons, internal controls, shell banks and corresponding banking relationships, wire transfers, record keeping, and anti-money laundering training and reporting requirements. Concerning customer due diligence, regulated entitles must update clients' due diligence information every three years for low risk business relationships and once every year for higher risk business relationships. The AMLR requires the retention of records for a period of at least five years from the date when all transactions relating to a one-off transaction or a series of linked transactions were completed, when the business relationship formally ended, or when the last transaction was carried out. However, there is no formal requirement for account files to be maintained for at least five years following the termination of an account or business relationship.

The POCCA (Amendment) 2006 mandates financial institutions and other providers of financial services to report suspected money laundering transactions including attempted transactions. The AMLR and the AMLTFCOP establishes procedures to identify suspicious transactions and report them to the financial intelligence unit (FIU). Obligated entities are protected from liability for reporting suspicious transactions. Reporting entities are required to create a clearly defined reporting chain for employees to follow when reporting suspicious transactions, and to appoint a reporting officer to receive such reports. The reporting officer must conduct an initial inquiry into the suspicious transaction and report it to the authorities if sufficient suspicion remains. Failure to report could result in criminal liability.

The POCCA mandates the creation of an FIU, the Reporting Authority. The Financial Investigation Agency (FIA) Act 2003 reorganized and renamed the FIU. The FIA's staff is comprised of a director, two senior police officers, one senior customs officer, a chief operating officer, a junior analyst, and an administrative assistant. A board is responsible for setting the policy framework under which the FIA operates. The board members include the Deputy Governor as chairperson, the Attorney General, the Financial Secretary, Managing Director/CEO of the Financial Services Commission, Director of the FIA, Commissioner of Police, and Comptroller of Customs.

The FIA is responsible for the collection, analysis, investigation, and dissemination of suspicious transaction reports (STRs). The FIA receives approximately 200 STRs annually. The FIA refers STRs that warrant further investigation to the Royal Virgin Islands Police Force (RVIPF), which is responsible for investigating drug trafficking, money laundering, and terrorism financing. In 2007, the FIA Act 2003 was amended to redefine the FIA's responsibilities to include investigation and analysis of any offense in relation to money laundering and terrorist financing. The amendment empowered the FIA to investigate matters relating to the breach of any domestic or international sanction prescribed by or under any enactment. It also provided the FIA authority to receive disclosures of suspected terrorist financing. However, a discrepancy exists with the FIA's ability to receive STRs related to the financing of terrorism. Technically, reporting institutions are to submit terrorist financing STRs directly to the RVIPF. It is unclear whether the RVIPF has an obligation to share the STR with the FIA. Presently, no terrorist financing STRs have been reported.

The FIA has the ability to request additional information from reporting institutions. The FIA also has a memorandum of understanding (MOU) with the FSC to facilitate information exchange between the two agencies. The FIA exchanges information with foreign counterpart FIUs, and does not require an MOU. The FIA has the authority to provide a written order to freeze a transaction for up to 72 hours, as well as has the authority to freeze a bank account on behalf of the Governor, Attorney General, the FSC, or a foreign FIU or law enforcement agency for a period of five days.

The POCCA (Amendment) 2008 replaced the Joint Anti-Money Laundering Coordinating Committee (JAMLCC) with the Joint Anti-Money Laundering and Terrorist Financing Advisory Committee (JALTFAC). The JALTFAC is comprised of the Managing Director of the FSC, the Attorney General, Commissioner of Police, Comptroller of Customs, Director of the FIA, and the Financial Secretary.

The JALTFAC also includes private sector stakeholders such as the Registered Agents Association, Compliance Officers Association, Bankers Association, Bar Association, and the Society of Trusts and Estate Practitioners. The purpose of the JALTFAC is to assist the FSC in formulating a code of practice; ensure reporting institutions are compliant with relevant AML/CTF measures; and keeping the BVI aware of AML/CTF developments locally and internationally.

The United Kingdom's Terrorism (United Nations Measures) (Overseas Territories) Order 2001 (TUNMOTO) and the Anti-Terrorism (Financial and Other Measures) (Overseas Territories) Order 2002 (ATFOMOTO) extend to the BVI. The Afghanistan (United Nations Sanctions) (Overseas Territories) Order 2001 and the al-Qaida and Taliban (United Nations Measures) (Overseas Territories) Order 2002 (ATUNMOTO) also apply to the BVI. Terrorist financing offenses are covered under the TUNMOTO under article 3 which makes it an offense for any person to invite another person to provide funds, or to receive and provide funds with the intention or knowledge that the funds may be used for the purpose of terrorism. Under the ATFOMOTO a person guilty of terrorist financing may be subject to imprisonment for a term not exceeding 14 years, to a fine, or to both, or on summary conviction to imprisonment for a term not exceeding six months, a fine not exceeding the statutory maximum or both. To date, there are no investigations of terrorism financing in the BVI.

The POCCA and the DTOA provide the ability to freeze or seize assets. Forfeiture is also covered by the POCCA and the DTOA upon conviction. The freezing and forfeiture of funds and property used for terrorist financing is covered by the ATUNMOTO, TUNMOTO, and the ATFOMOTO. The Governor of the BVI is responsible for executing freeze orders related to terrorist financing. Reporting institutions are advised to monitor relevant websites for names of suspected terrorists and related organizations. No specific guidance has been issued to outline reporting institutions obligations to freeze funds of designated terrorists and terrorist organizations.

The Office of the Director of Public Prosecution (ODPP) is responsible for obtaining forfeiture, charging and restraint orders, and the prosecution of all money laundering and other criminal investigations. Currently, there are two ongoing money laundering investigations. The last money laundering conviction was obtained in 2003. In May 2008, the GOBVI confiscated $45 million in an alleged international money laundering case from the Bermuda based IPOC International Growth Fund. The IPOC case gained international notoriety with allegations that IPOC was a money laundering front with ties to Russia's Telecommunications Minister, among others. Tried in the BVI, the case involved IPOC and three BVI IBCs. A 17-month investigation by BVI authorities revealed a complex web of irregularities with false parties to agreements, allegedly forged signatures, and falsified documents exhibiting that the three BVI IBCs received payments from third parties for services rendered; however, those companies had not provided the services claimed, or had not made the payments. As a result, these entities plead guilty to furnishing false information and obstruction of justice. The BVI intends to confiscate the entire funds of IPOC within its jurisdiction and share the forfeited assets with the Government of Bermuda. The BVI IBCs will be dissolved no later than April 2009.

The BVI is a member of the Caribbean Financial Action Task Force (CFATF), a FATF-style regional body and underwent a mutual evaluation in February 2008. As a result the government enacted anti-money laundering legislation that requires financial institutions to identify the beneficial owners of companies, cut ties with shell banks and refuse requests to open anonymous accounts. This legislation helps the country comply with the European Union's Third Money Laundering Directive. The BVI is an observer to the Offshore Group of Supervisors, and the FIA is a member of the Egmont Group. The BVI is subject to the 1988 UN Drug Convention and, as a British Overseas Territory, has implemented measures in accordance with this convention and the UN Convention against Transnational Organized Crime. The UK extended the application of the UN Convention against Corruption to the BVI in October 2006. The U.S. and the British Virgin Islands established a Tax Information Exchange Agreement (TIEA) in 2006. Application of the U.S.-UK Mutual Legal Assistance Treaty (MLAT)

concerning the Cayman Islands was extended to the BVI in 1990. The FIA handles MLAT and other legal assistance requests after they have been reviewed by the Office of the Attorney General.

The Government of the British Virgin Islands (GOBVI) made substantial efforts to bolster their AML/CTF regime during 2008. However, the GOBVI should consider revising money laundering and terrorist financing penalties to dissuade criminals and terrorists from exploiting the territory. The GOBVI should specify that the FIA directly receive STRs related to terrorism financing. The BVI should ensure that designated nonfinancial businesses and professions adhere to the provisions of its AML/CTF regulations particularly with the reporting of STRs. The GOBVI should ensure that there are a sufficient number of regulators and examiners to exercise effective due diligence, regulation, and inspections of its 446, 865 active BVI companies in a manner compliant with international standards.

Bulgaria

The Government of Bulgaria (GOB) needs to seriously strengthen its anti-money laundering regime. While Bulgaria is not considered an important regional financial center or an offshore financial center, it is significant in terms of its geographical position, its well-developed financial sector relative to other Balkan countries, its relatively lax regulatory control, and its government tolerance of corruption and failure to strictly enforce anti-money laundering (AML) laws. Moreover, Bulgaria is a major transit point for the trafficking of drugs and persons into Western Europe, generating criminal proceeds that are subsequently laundered in Bulgaria. Bulgaria is primarily a cash economy, thereby making it more difficult to trace illicit money flows. ATM and credit card fraud remain serious problems. Tax fraud is prevalent. Smuggling remains a problem, reportedly sustained by corrupt Bulgarian businessmen and politicians. Organized crime groups are moving into legitimate business operations, making it difficult to determine the origins of their wealth. While tourism and construction formed the basis for the country's economic revival in recent years, they have also become favorite money laundering routes for organized crime groups with suspected ties to politicians.

Since its admission to the European Union (EU) in 2007, Bulgaria has faced constant criticism and pressure from the European Commission (EC) regarding its failure to effectively combat corruption. Public officials, watchdog institutions, and journalists who challenge organized crime operations often face intimidation. Corruption, fraud, and organized crime are such pervasive problems in Bulgaria that the EU stripped the country of 220 million Euros (approximately $285,200,000) of funds in November 2008 and said Bulgaria might lose another 340 million Euros (approximately $440,700,000) if it failed to curb corrupt practices and political interference in funding processes by the end of 2009. Although Bulgaria has launched several investigations into government officials and businessmen suspected of funds fraud, it has failed to convict a single senior official of graft and has jailed only one organized crime leader.

Despite the prevalence of corruption and weak enforcement of AML laws, Bulgaria has managed to make some progress in 2008. Facing sharp EU, U.S. and civil society criticism, the Bulgarian government finally closed all duty free shops and petrol stations at Bulgaria's land borders in July 2008. These establishments had been suspected to be major centers for contraband, tax evasion, and money laundering. In October 2008, after repeated requests by the U.S. and EU, and after protracted delays, the government decided to mandate that the actual amount of a cash transaction be listed on reporting forms. This closed an important loophole in AML legislation that had previously served to facilitate money laundering. Despite these improvements, the GOB's AML efforts still need substantial intensification.

Article 253 of the Bulgarian Penal Code criminalizes money laundering related to all crimes. As such, drug-trafficking is but one of many recognized predicate offenses. Amendments made to the Penal Code in 2006 increase penalties (including in cases of conspiracy and abuse of office), clarify that predicate crimes committed outside Bulgaria can support a money laundering charge brought in

Bulgaria, and allow prosecution on money laundering charges without first obtaining a conviction for the predicate crime.

The Law on Measures against Money Laundering (LMML) is the legislative backbone of Bulgaria's AML regime. Adopted in 1998, the LMML has since been amended several times, most recently in 2008. The many revisions to the law, though often in the right direction, have rendered the law less comprehensible and hence less effective. Bulgaria has strict and wide-ranging banking, tax, and commercial secrecy laws that limit the dissemination of financial information absent the issuance of a court order. The 2006 amendments to the Law on Credit Institutions facilitate the investigation and prosecution of financial crimes by giving the Prosecutor General the right to request financial information from banks without a court order in cases involving money laundering and organized crime.

In response to pressure from the EU, in 2006, Bulgaria's Parliament tightened the LMML with further amendments. These amendments expand the definition of money laundering and the list of reporting entities; outlaw anonymous bank accounts; expand the definition of "currency"; and require the disclosure of the source of currency exported from the country. Under the LMML, 30 categories of entities, including lawyers, real estate agents, auctioneers, tax consultants, and security exchange operators are required to file suspicious transaction reports (STRs). The banking sector, with some key exceptions, has substantially complied with the law's filing requirement. Reporting by other sectors, in particular reporting related to the explosion of real estate transactions (e.g., notaries and real estate agents), has been much lower.

The Law on Administrative Violations and Penalties, as amended in 2005, establishes the liability of legal persons (companies) for crimes committed by their employees.

Bulgaria's financial intelligence unit (FIU), the Financial Intelligence Directorate (FID) within the State Agency for National Security (DANS) is the main administrative unit for collecting and analyzing information on suspected money laundering transactions. The FID-DANS does not participate in criminal investigations. In the past year, FID has had its powers severely limited. Prior to December 2007, Bulgaria's FIU was a fully independent agency operating under the Ministry of Finance (MOF), with the independence of its director guaranteed by the LMML. It had the authority to perform onsite compliance inspections, obtain information without a court order, share all information with law enforcement, and receive reports of suspected terrorist financing. However, on December 11, 2007, the Parliament passed legislation that came into force on January 1, 2008, which limits the FID's effectiveness and autonomy. This law, the Act on the State Agency for National Security, establishes DANS as the new national intelligence agency. The law also restructures the FID by changing its status from an independent agency within the MOF to a directorate within the DANS; consequently, the FID is no longer an individual legal entity with its own budget. Some of the FID's previous authorities were removed from the law and included only in regulations, further diminishing the FID's status. Other authority was assigned to the director of DANS, but not expressly to the FID, thereby limiting its ability to compel legal compliance by banks. In addition, discrepancies between the LMML and the law creating DANS create uncertainty regarding the FID's inspection and sanctioning authorities, including its ability to perform AML on-site inspections. In addition, the analytical capacity of FID is not precisely defined: the DANS law permits the FIU to acquire and handle national security-related information, but financial crimes information is not necessarily of national security importance. From January 1 to May 1, 2008, the Egmont Group of FIUs temporarily suspended Bulgaria's access to its secure information exchange system, pending a review of FID's authorities under the new legislation.

As of September 2008, the FID-DANS conducted 46 on-site inspections and issued 44 penal decrees totaling 119,500 BGN (approximately $78,826), as compared with 83 such inspections of banking and nonbanking institutions as of October 2007. As of September 2008, there was only one on-site

inspection of a bank, and the bank challenged the powers of FID-DANS inspectors to ask for information necessary for completing the inspection. FID-DANS proposed the issuance of three criminal citations related to that on-site inspection for refusal to provide access to bank documents and clients' files.

Banks and the 29 other reporting entities under the LMML are required to apply "know your customer" (KYC) standards. Since 2003, all reporting entities are required to ask for the source of funds in any transaction greater than 30,000 BGN (approximately $22,500) or foreign exchange transactions greater than 10,000 BGN (approximately $7,500). Reporting entities are also required to notify the FID-DANS of any cash payment greater than 30,000 BGN ($22,500). Because of inconsistent interpretation of the cash reporting requirement, some believe it covers only cash deposits, allowing a loophole to exist to the benefit of money launderers by leaving an unknown percentage of large cash withdrawals or exchanges unreported. As mentioned previously, as of January 1, 2009, Bulgarian banks will have to include the actual amount of all cash deposits above the 30,000 BGN (approximately $22,500) cash transaction reporting (CTR) threshold. This is in contrast to the previous requirement mandating banks report only that the transaction occurred but not the actual amount.

The LMML obligates financial institutions to a five-year record keeping requirement and provides a safe harbor to reporting entities. Penal Code Article 253B was enacted in 2004 to establish criminal liability for noncompliance with LMML requirements.

Bearer shares can be issued by joint stock companies, although not by banks or state companies. There are no limitations on the issuance. The identity of the first owner is registered; however, subsequent sales are not recorded. The GOB indicated these share are rarely issued.

Bulgaria does not systematically track cross-border electronic currency transactions, thereby making Bulgaria an attractive entry point to funnel money into the European financial system. During the year, the FID-DANS noted an increase in flows of money through Bulgaria. Bulgaria's Customs Agency collects criminal intelligence from its officers at points of entry, reviews cash reporting documents, and requests assistance from foreign partners to determine whether cash couriers are engaged in criminal activity. Customs officers have intercepted enormous quantities of cash in hidden compartments in cars.

Cash transactions in Bulgaria have grown an average of 46 percent per year over the past three years (while the economy has grown, on average, about seven percent). In 2008, the FID-DANS received 344,897 CTRs, but only 592 STRs for a total value of 257,459,070 euros (approximately $347,569,740). Banks submitted 515 of the STRs. Given the scale of growth of cash transactions over the 30,000 BGN (approximately $22,500) reporting threshold, the number of STRs is exceptionally low. Some banks in Bulgaria have not filed any suspicious transaction reports in the past three years, with no clear consequence for the vast majority of them. Other locally-owned Bulgarian banks do inordinate volumes of their business in cash. Despite the cash intensive nature of Bulgaria's economy, the large volume of cash transactions being observed in Bulgarian business is disproportionate to ordinary, customary, and normal practices.

Historically lower rates of reporting compliance by exchange bureaus, casinos, and other nonbank financial institutions can be attributed to numerous factors, including a lack of understanding of, or respect for legal requirements; lack of inspection resources; and the general absence of effective regulatory control over the nonbank financial sector. According to its most recent evaluation of Bulgaria conducted in 2007, the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), a Financial Action Task Force-style regional body, noted deficiencies in Bulgaria's STR reporting regime, citing (among other problems) a lack of reporting from nonbanking financial institutions. During 2008, FID-DANS noted that while the compliance by nonbank entities remained low, the quality of their STRs

improved. As of September 2008, the FID-DANS inspected eight exchange offices, imposing fines in seven cases for a total of 20,000 BNG (approximately $13,000) for failure to identify clients or request declarations on the origin of funds, and for not filing STRs.

DANS and the Prosecution Service drafted an instruction regulating interaction mechanisms between the two entities, including elements on interaction of FID-DANS and the Prosecutors Office. The instruction also establishes a permanent Contact Group of four prosecutor sector heads within the Supreme Prosecutors Office of Cassation and four directors from DANS, including the FID Director, to coordinate and manage cooperation between the two entities. DANS also drafted another instruction regulating interaction mechanisms between DANS and the Interior Ministry. These two instructions, signed by the Chairman of DANS and the Prosecutor General and Minister of Interior, respectively, replace the prior instructions on cooperation mechanisms.

Although case law remains weak, there has been an increase in the prosecution of money laundering cases. In October 2006, the courts rendered the country's first two convictions for money laundering. Bulgaria still has failed to convict a major high-profile organized crime figure, and most money laundering cases involve relatively small amounts of money and lower level crime figures. In the first half of 2008, prosecutors worked on 106 pre-trial investigations compared to 54 for the same period of 2007, or a 51 percent increase in caseload. During this period, prosecutors filed five indictments in court (equal to the number of indictments in the first half of 2007), against eight persons (as compared to five persons in the first half of 2007). There were two convictions (as compared to four in the first half of 2007) and no acquittals. Bulgaria's location as a crossroads for the entry into Europe of southwest Asian narcotics suggests that drug monies flow as well, as do proceeds from trafficking in persons and other crime activities. Money laundering has not figured prominently in legal cases against such perpetrators, though the Ministry of Interior is eager to strengthen its capacity in this area.

Although there are few indications of terrorist financing directly connected with Bulgaria, the possibility remains that terrorism-related funds can transit Bulgarian borders through cash couriers and other informal mechanisms. In 2008, FID-DANS received only one STR in the amount of 1,681,248 euros (approximately $2,269,685) related to possible terrorist financing. To date, no suspected terrorist assets have been identified, frozen, or seized by Bulgarian authorities. Article 108a of the Penal Code criminalizes terrorism and terrorist financing. Article 253 of the Criminal Code qualifies terrorist acts and terrorist financing as predicate crimes under the "all crimes" approach to money laundering. In February 2003, the GOB enacted the Law on Measures Against Terrorist Financing (LMATF), which links counterterrorism measures with financial intelligence, and compels all covered entities to report any suspicion of terrorist financing or pay a penalty of up to 50,000 BGN (approximately $37,500). The law authorizes the FID to use its resources and financial intelligence to combat terrorist financing along with money laundering. Bulgaria's STR reporting requirements with regard to terrorist financing are still deficient, however, lacking a reporting obligation covering funds suspected to be linked to terrorists or terrorist financing.

Under the LMATF, the GOB may freeze the assets of a suspected terrorist for 45 days. Key players in the process of asset freezing and seizing, as prescribed in existing law, include the MOI, DANS, Council of Ministers, Supreme Administrative Court, Sofia City Court, and the Prosecutor General. The FID-DANS and the Bulgarian National Bank circulate the names of suspected terrorists and terrorist organizations found on the UNSCR 1267 Sanctions Committee's Consolidated List, the list of Specially Designated Global Terrorists designated by the U.S. pursuant to Executive Order 13224, and those designated by the relevant EU authorities.

Although alternative remittance systems may operate in Bulgaria, their prevalence is unknown, and there are no reported initiatives underway to address them. In general, regulatory controls over nonbank financial institutions are weak, with some of those institutions engaging in banking activities

absent any regulatory oversight. Some anecdotal evidence suggests that charitable and nonprofit legal status is occasionally used to conceal money laundering.

The Bulgarian Penal Code provides legal mechanisms for forfeiting assets (including substitute assets in money laundering cases) and instrumentalities. Both the money laundering and the terrorist financing laws include provisions for identifying, tracing, and freezing assets related to money laundering or the financing of terrorism. A civil asset forfeiture law, targeted at confiscation of illegally acquired property, came into effect in March 2005. The law permits forfeiture proceedings to be initiated against property valued in excess of 60,000 BGN (approximately $45,100) if the owner of the property is the subject of criminal prosecution for enumerated crimes (terrorism; drug-trafficking; human trafficking; money laundering; bribery; major tax fraud; and organizing, leading, or participating in a criminal group); and a reasonable assumption can be made that the property was acquired through criminal activity. As required by the law, an Assets Forfeiture Commission was established and became operational in 2006. The Commission has the authority to institute criminal asset identification procedures, as well as request from the court both preliminary injunctions, and ultimately, the forfeiture of assets. Since its establishment, the Commission has faced strong criticism and demands for its closure from both government officials who question its effectiveness and politically connected businessmen allegedly protecting their interests. Initial indications show that the Commission is starting to become effective despite the fact that the process is slow, requires preliminary criminal prosecution against the owner, and often results in assets being transferred to relatives or significantly undervalued. As of October 2008, the Commission froze five million BGN (approximately $3,300,000). During this period, the Commission noted that first instance courts in six cases (approximately 80 percent of the cases) granted claims for 2.8 million BGN (approximately $1,800,000). In one case, the Commission accepted a conviction from a U.S. federal court as the basis for asset freezing and forfeiture proceedings in Bulgaria.

In September 2007, the United States and Bulgaria signed a mutual legal assistance treaty (MLAT), implementing the U.S.-EU Mutual Legal Assistance Agreement, which has yet to come into force. As of October 2007, the FID had bilateral memoranda of understanding (MOU) regarding information exchange relating to money laundering with 28 countries. The FID-DANS is authorized by law to exchange financial intelligence on the basis of reciprocity without the need of an MOU. As of October 2007, the FID-DANS sent 261 requests for information to foreign FIUs and received 54 requests for assistance from foreign FIUs.

Bulgaria participates in MONEYVAL, and the FID Director is the current Chairman of MONEYVAL. The FID-DANS is a member of the Egmont Group. Bulgaria is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption.

Until December 2007, Bulgaria's legislative framework was largely viewed as consistent with international AML standards. The Act on the State Agency for National Security compromised the FID's independence and investigatory mandate. It is essential that the Government of Bulgaria rectify these shortcomings. It must clarify and strengthen the FID's inspection and sanctioning authorities. The GOB should also take steps to improve and tighten its regulatory and reporting regime, particularly with regard to nonbank sectors, bearer shares, and cash payments, including cash withdrawals and exchanges, cross border transactions, and real estate transactions. The GOB should correct the deficiencies in its STR system regarding suspected terrorist financing. The GOB should improve the consistency of its customs reporting enforcement and should also establish procedures to identify the origin of funds used to acquire banks and businesses during privatization. Interagency cooperation should be streamlined to ensure effective implementation of Bulgaria's anti-money laundering and counterterrorist financing regime, and to improve prosecutorial effectiveness in money laundering, trafficking, narcotics, and terrorist financing cases. To improve judicial review of money laundering cases, the Government should enhance the capacity of judges regarding money laundering

and promote a consistent interpretation of money laundering and asset forfeiture laws. In order to remove the risk that criminal interests are able to regain possession of confiscated goods, the GOB should also clarify the authorities of the Asset Forfeiture Commission so as to provide a mechanism to manage and dispose of confiscated properties.

Burma

Burma is a major drug-producing country and its economy remains dominated by state-owned entities, including the military. Drug trafficking and human trafficking are the major sources of money laundering in Burma. Wildlife, gems, timber, and other contraband flow through Burma and are additional sources of money laundering, as is public corruption. Agriculture and extractive industries, including natural gas, mining, logging and fishing provide the major portion of national income, with heavy industry and manufacturing playing minor roles. The steps Burma has taken over the past several years have reduced vulnerability to drug money laundering in the banking sector. However, with an underdeveloped financial sector and large volume of informal trade, Burma remains a country where there is significant risk of drug money being funneled into commercial enterprises and infrastructure investment. Regionally, value transfer via trade is of concern and hawala/hundi networks frequently use trade goods to provide countervaluation. Burma's border regions are difficult to control and poorly patrolled. In some remote regions active in smuggling, there are continuing ethnic tensions with armed rebel groups that hamper government control. Collusion between traffickers and Burma's ruling military junta, the State Peace and Development Council (SPDC), allows organized crime groups to function with virtual impunity. Although progress was made in 2008, the criminal underground faces little risk of enforcement and prosecution. Corruption in business and government is a major problem. Burma is ranked 178 out of 180 countries in Transparency International's 2008 Corruption Perception Index.

The Government of Burma (GOB) has addressed some key areas of concern identified by the international community by implementing some anti-money laundering measures. In October 2006, the Financial Action Task Force (FATF) removed Burma from the FATF list of Non-Cooperative Countries and Territories (NCCT). To ensure continued effective implementation of reforms in Burma, the FATF, in consultation with the Asia/Pacific Group on Money Laundering (APG)—the relevant FATF-style regional body (FSRB) continues to monitor developments there for a period of time after de-listing. In 2008, the FATF advised the GOB to enhance regulation of the financial sector, including the securities industry, and to ensure that the GOB responds adequately to any foreign requests for cooperation.

Burma underwent a mutual evaluation by the APG in July 2008. This evaluation assessed Burma's AML/CTF regime as noncompliant or only partially compliant in all but four of the FATF 49 recommendations, a clear indication that Burma remains highly vulnerable to money laundering and terrorism finance threats. Key findings in the report included the observation that Burma has no law specifically penalizing terrorism as a separate crime, and has not enacted a law specifically criminalizing terrorist financing and designating it as one of the predicate offences to money laundering. In addition, the prevalent use of the U.S. dollar in Burma makes cash courier/currency smuggling of U.S. dollars an attractive method of laundering illicit proceeds.

Burma enacted a "Control of Money Laundering Law" in 2002. It also established the Central Control Board of Money Laundering in 2002 and a financial intelligence unit (FIU) in 2004. The law created reporting requirements to detect suspicious transactions. It set a threshold amount for reporting cash transactions by banks and real estate firms, albeit at a high level of 100 million kyat (approximately $75,000). Between 2004 and August 2008, more than 86,000 cash transaction reports were filed. However, the FIU lacks a separate budget and its independence is hampered by the operational role of the Central Control Board (CCB) in Suspicious Transaction Reporting (STR) processing. The GOB's

2004 anti-money laundering measures amended regulations instituted in 2002-2003 that set out 11 predicate offenses, including narcotics activities, human trafficking, arms trafficking, cyber-crime, and "offenses committed by acts of terrorism," among others. In 2004 the GOB added fraud to the list of predicate offenses, established legal penalties for leaking information about suspicious transaction reports, and adopted a "Mutual Assistance in Criminal Matters Law." The 2003 regulations, further expanded in 2006, require banks, customs officials and the legal and real estate sectors to file STRs and impose severe penalties for noncompliance.

The GOB established a Department against Transnational Crime in 2004. Its mandate includes anti-money laundering activities. It is staffed by police officers and support personnel from banks, customs, budget, and other relevant government departments. In response to a February 2005 FATF request, the GOB submitted an anti-money laundering implementation plan and produced regular progress reports in 2006, 2007, and 2008. In 2005, the government also increased the size of the FIU to 11 permanent members, plus 20 support staff. In August 2005, the Central Bank of Myanmar issued guidelines for on-site bank inspections and required reports that review banks' compliance with anti-money laundering (AML) legislation. Since then, the Central Bank has sent teams to instruct bank staff on the new guidelines and to inspect banking operations for compliance. However, there are significant inadequacies in the Control of Money Laundering Law and regulations for a number of key preventive measures including the obligation to identify persons who either control or are the actual beneficial owners of corporations and the absence of application of customer due diligence to existing customers or to politically exposed persons (PEPs).

In 2007, the Burmese Government amended its "Control of Money Laundering Law" to expand the list of predicate offences to all serious crimes to comport with FATF's recommendations. In July 2007, the Central Control Board issued five directives to bring more nonbank financial institutions, including dealers in precious metals and stones, under the AML/CTF compliance regime. However, there is no law or regulation that requires the licensing or registration of informal money remitters (Hundi), other than as financial institutions. In March 2008, the CCB brought additional nonbank financial institutions, including the Andaman Club Resort Hotel and gems and jade trading companies (both wholesale and retail) under the AML/CTF compliance regime. However, there is no law or regulation that requires the licensing or registration of informal money remitters (Hundi), (other than as financial institutions) or to Designated Non-Financial Businesses and Professions. The Central Bank also required banks and financial institutions to maintain all records and documents related to customer accounts and transactions for a minimum of five years. Currently, there are 4 state-owned banks, 15 domestic private banks and a few nonbank financial institutions, which include a state-owned insurance enterprise, a state owned small loan enterprise, and a private owned leasing company.

The Law Relating to Forming Organizations (LRPO) governs Non-Profit Organizations (NPOs) of which there are three hundred and two registered under this law, seventy-eight of which have international connections. There has been no comprehensive review of the LRFO or the NPO sector including any review to assess the vulnerabilities to terrorist financing, nor is there any requirement for NPOs to maintain and make their records available to public authorities.

As of August 2008, a total of 1,495 STRs had been received. In 2007, nine cases were identified as potential money laundering investigations. As of August 2008, the FIU received 444 STRs, of which seven cases were identified as potential money laundering investigations. The FIU has investigated four cases to date, two of which were sent to the courts for prosecution. According to the 2008 Asia Pacific Group on Money Laundering (APG) Mutual Evaluation Report, there has been only one conviction for money laundering itself since 2004 despite twenty-three money laundering investigations and fifty-four people having been convicted for predicate crimes under the "Control of Money Laundering Law.

The United States maintains the anti-money laundering measures it adopted against Burma in 2004, identifying the jurisdiction of Burma and two private Burmese banks, Myanmar Mayflower Bank and Asia Wealth Bank, to be "of primary money laundering concern" pursuant to Section 311 of the 2001 USA PATRIOT Act. These measures prohibit U.S. banks from establishing or maintaining correspondent or payable-through accounts in the United States for or on behalf of Myanmar Mayflower and Asia Wealth Bank and, with narrow exceptions, for all other Burmese banks. Myanmar Mayflower and Asia Wealth Bank had been linked directly to narcotics trafficking organizations in Southeast Asia. In March 2005, following GOB investigations, the Central Bank of Myanmar revoked the operating licenses of Myanmar Mayflower Bank and Asia Wealth Bank, citing infractions of the Financial Institutions of Myanmar Law. The two banks no longer exist. In August 2005, the Government of Burma also revoked the license of Myanmar Universal Bank (MUB), and convicted the bank's chairman under both the Narcotics and Psychotropic Substances Law and the Control of Money Laundering Law. Under the money laundering charge, the court sentenced him to one 10-year and one unlimited term in prison and seized his and his bank's assets.

The United States also maintains other sanctions on Burma, which include bans on certain importations, new investment, and certain financial transactions, as well as a visa ban on selected individuals. Under the Block Burmese JADE (Junta's Anti-Democratic Efforts) Act of 2008, the Burmese Freedom and Democracy Act of 2003, and several Executive Orders, the United States bans the transfer of funds and other provision of financial services to Burma by any U.S. person, freezes assets of the ruling junta and other Burmese individuals and entities, and prohibits the import of all Burmese-origin goods into the United States (with tighter restrictions on jadeite and rubies). Additional U.S. laws—such as the Narcotics Control Trade Act, the Foreign Assistance Act, the International Financial Institutions Act, the Export-Import Bank Act, the Export Administration Act, the Customs and Trade Act, and the Tariff Act (19 USC 1307)—place further restrictions on financial transactions with Burma. Other U.S. sanctions, such as visa bans on certain individuals affiliated with the military regime, also apply to Burma.

In September 2008, the United States Government identified Burma as one of three countries in the world that had "failed demonstrably" to meet its international counternarcotics obligations. On November 13, 2008, the Office of Foreign Assets Control in the Department of the Treasury named 26 individuals and 17 companies tied to Burma's Wei Hsueh Kang and the United Wa State Army (UWSA) as Specially Designated Narcotics Traffickers pursuant to the Foreign Narcotics Kingpin Designation Act (Kingpin Act). Wei Hsueh Kang and the UWSA were designated by the president as Foreign Narcotics Kingpin on June 1, 2000 and June 2, 2003 respectively.

Burma became a member of the Asia Pacific Group on Money Laundering in 2006. The GOB is a party to the 1988 UN Drug Convention. Over the past several years, Burma has expanded its counternarcotics cooperation with other states. The GOB has bilateral drug control agreements with India, Bangladesh, Vietnam, Russia, Laos, the Philippines, China, and Thailand. These agreements include cooperation on drug-related money laundering issues. In July 2005, the Myanmar Central Control Board signed an MOU with Thailand's Anti-Money Laundering Office governing the exchange of information and financial intelligence. The government signed a cooperative MOU with Indonesia's FIU in November 2006.

Burma is a party to the UN Convention against Transnational Organized Crime and to the UN Convention for the Suppression of the Financing of Terrorism. Burma is not a party to the UN Convention on Corruption. Burma signed the Treaty on Mutual Legal Assistance in Criminal Matters among Like-Minded ASEAN Member Countries in January 2006, and deposited its instrument of ratification with the Attorney General of Malaysia in January 2009.

The Government of Burma has in place a framework to allow mutual legal assistance and cooperation with overseas jurisdictions in the investigation and prosecution of serious crimes. To fully implement

a strong anti-money laundering/counterterrorist financing regime, Burma must provide the necessary resources to administrative and judicial authorities who supervise the financial sector so they can apply and enforce the government's regulations to fight money laundering successfully. Burma must also continue to improve its enforcement of the new regulations and oversight of its financial sector, including its banks, its DNFBPs as well as its NPOs. The GOB should end all government policies that facilitate the investment of drug money and proceeds from other crimes into the legitimate economy. The reporting threshold for cash transactions should be lowered to a realistic threshold that fits the Burmese context and the FIU should become a fully funded independent agency that is allowed to function without interference. Customs should be strengthened and authorities should monitor more carefully the misuse of trade and its role in informal remittance or hawala/hundi networks. Burma should become a party to the UN Convention against Corruption. The GOB should take serious steps to combat smuggling of contraband and its link to the pervasive corruption that permeates all levels of business and government. The GOB should criminalize the financing of terrorism. Finally, the GOB should adhere to all laws and regulations that govern anti-money laundering and terrorist financing to which it is committed by virtue of its membership in the UN and the APG.

Cambodia

Cambodia is neither an important regional financial center nor an offshore financial center. The major sources of money laundering are widespread human trafficking and exploitation, drug trafficking, and corruption. Cambodia serves as a transit route for drug trafficking from the Golden Triangle to international drug markets such as Vietnam, mainland China, Taiwan, and Australia. Cambodia's fledgling anti-money laundering regime, a cash-based economy with an active informal banking system, porous borders with attendant smuggling, limited capacity of the National Bank of Cambodia (NBC) to supervise a rapidly expanding banking sector, and widespread corruption continue to contribute to a significant money laundering risk. The vulnerability of Cambodia's financial sector is further exacerbated because of the intersection of the casino and banking interests with four companies having whole or partial shares in both banks and casinos. In addition, terrorist financing is a significant risk in Cambodia as highlighted the 2003 case involving Jemaah Islamiyah (JI). However, with the 2007 enactment of the "Law on Anti-Money Laundering and Combating the Financing of Terrorism" (AML/CTF) and the subsequent May 2008 implementing regulation, and the enactment of the "Law on Counter Terrorism" Cambodia has created a foundation to combat acts of money laundering and terrorist financing within the banking sector. Additional implementing regulations are needed to bring all designated nonfinancial businesses and professions (DNFBPs) into compliance with reporting requirements established in the AML/CTF law.

The AML/CTF law was promulgated in June 2007 and provides the framework for the Cambodian Financial Intelligence Unit (CAFIU) to exert control over banks and DNFBPs, such as casinos and realtors and entities to be designated by the CAFIU. The NBC is making strides to regulate large or suspicious financial transactions. There were two suspicious cases reported as of the third quarter of 2008 and investigations are ongoing. The Prakas (implementing regulation) on the AML/CTF law was issued on May 30, 2008, and was soon to put into force. The new Prakas places a wide range of AML/CTF obligations on banks and financial institutions that are regulated by the NBC. Since then, the CAFIU has been working with the Ministry of Interior, Ministry of Justice, and other relevant ministries to take cooperative action, ranging from identifying and reporting suspicious financial transactions, raising awareness, to lodging judicial complaints to the Ministry of Justice for court action on possible cases. The Prakas requires all reporting entities regulated by the NBC to report on a regular basis and to establish internal control systems for AML/CTF procedures to be fully compliant with the law. However, additional decrees are necessary to establish reporting procedures and formats for DNFBPs to fully implement the AML/CTF law. The Ministry of Interior has a legal responsibility for general oversight of casinos operations and providing security; however, in practice it exerts little

supervision. The Ministry of Interior is authorized to investigate cases of suspicious transactions reported to it by the CAFIU.

Cambodia's banking sector is relatively small, yet rapidly expanding, with 25 commercial banks (an increase of ten in the last year); six specialized banks; 18 registered micro-finance institutions (MFIs); 3,808 money exchangers (556 in Phnom Penh and 3,252 in the provinces); and 26 registered and roughly 60 unregistered NGO credit operators. Bank operations are widely made on a cash basis and predominantly in U.S. dollars. Recently, the Royal Government of Cambodia (GOC) encouraged the use of the national currency (the riel) in lending and borrowing. Despite an increase in the use of banking and finance systems, overall lending and banking activities remain low due to lack of trust and prohibitive interest rates on loans. Increased borrowing and loans are due mainly to expansion in the construction and real estate sectors. Economists note that while a typical country would have a bank deposit to GDP ratio of roughly 60 percent, Cambodia's ratio is only 26.2 percent (August 2008), low even by developing economy standards. Cambodia's banking system is highly consolidated, with two banks—Canadia Bank and ANZ Royal—accounting for more than 30 percent of all bank deposits. In addition to banks, individual and legal persons can undertake foreign exchange provided they register with the NBC.

The NBC has regulatory responsibility for the banking sector, and it audits and inspects individual banks on-site on an annual basis to ensure full compliance with laws and regulations. Moreover, off-site investigations can be made on a daily, weekly, or monthly basis contingent upon each individual case. The AML/CTF law requires that banks and other financial institutions report transactions over 40,000,000 riel (approximately U.S. $10,000). However, large cash reporting is not yet implemented due to lack of a database within the CAFIU. While there are no reports to indicate that banking institutions themselves are knowingly engaged in money laundering, until the CAFIU was established, government audits would likely not have been a sufficient deterrent to money laundering through most Cambodian banks. With increased political stability and the gradual return of normalcy in Cambodia after decades of war and instability, bank deposits have risen on average by about 41.6 per cent per year from 2004 to 2007. From January to August of 2008, deposits grew on average by 52 percent, due in part to new increased deposit requirements. The financial sector shows some signs of deepening as domestic business activity continues to increase in the handful of urban areas. Foreign direct investment, while limited, continues to grow.

Cambodia lacks meaningful statistics on the extent of financial crime that exists and only a few crime statistics and limited open source information is available to evaluate the major sources of illicit funds. Despite the establishment of the CAFIU, some larger-scale money laundering in Cambodia may also flow through informal banking activities and/or business activities. The Cambodian authorities consider that there are informal money or value transfer operations carried out by money changers, or individuals within Cambodia or across borders. The black market in Cambodia for smuggled goods, including drugs and imported substances for local production of the methamphetamine ATS, is notable. Most of the smuggling is intended to circumvent official duties and evade tax obligations and involves items such as fuel, alcohol optical disks, and cigarettes. Some government officials and their private sector associates have some control over the smuggling trade and its proceeds. Cambodia's economy is cash-based and largely dollarized, and the smuggling trade is usually conducted in U.S. dollars. Such proceeds are rarely transferred through the banking system or other financial institutions. Instead, they are readily channeled into land, housing, luxury goods or other forms of property. Cambodia's urban real estate sector, fueled by foreign investment, has witnessed rapid growth and soaring prices in recent years.

The CAFIU is under the control and financing of the NBC with a Permanent Secretariat working under the supervision of a Board of Directors composed of one senior representative each from the NBC, Council of Ministers, and the Ministries of Economy and Finance, Justice, and Interior. Under Article 5 of the Prakas on AML/CTF, banks and financial institutions are required to conduct customer

due diligence when carrying out an occasional or one-off transaction that involves a sum in excess of U.S. $10,000 (or 40 million riel or foreign currency equivalent) or a wire transfer that involves a sum in excess of U.S. $ 1,000 (or 4 million riel or other equivalent foreign currency). The CAFIU has also offered "Know Your Customer" and other training to banking institutions to inform them of their obligations under the new AML/CTF regime.

The CAFIU has the authority to apply anti-money laundering requirements to DNFBPs such as casinos and other intermediaries, such as lawyers, notaries, and accountants. The major nonbank financial institutions in Cambodia are the casinos, which the authorities have noted are particularly vulnerable to money laundering. By law, foreigners, but not Cambodian nationals, are allowed to gamble in casinos. The regulation of casinos falls under the jurisdiction of the Ministry of Interior, although the Ministry of Economy and Finance issues casino licenses and the CAFIU has the authority to receive and disseminate reports, including suspicious transaction reports, on casino financial transactions and cooperate with casino regulators on AML/CTF. There are currently 27 operational licensed casinos in Cambodia, a few other licensed casinos are under construction, and there are an unrecorded number of small-sized gambling houses. Most casinos are located along Cambodia's north-west border with Thailand and along the Cambodia's southeastern border with Vietnam. However, one can also find casinos and so-called 'gambling houses' at hotels in major cities and towns. There is one large casino in Phnom Penh that has avoided the regulation that all casinos be at least 200 kilometers from the capital city. Casino patrons placing small bets simply hand-carry their money across borders, while others use either bank transfers or junket operators. Cambodian casinos have accounts with major Thai or Vietnamese banks and patrons can wire large amounts of money to one of these foreign accounts. After a quick phone call to verify the transfer, the Cambodian casino issues the appropriate amount in chips. Casinos also work with junket operators who, despite their name, only facilitate money transfers and do not serve as travel or tour operators. Players deposit money with a junket operator in Vietnam or Thailand, the casino verifies the deposit and issues chips to the player-typically up to double the amount of the deposit. After the gambling session ends, the junket operator then has 15 days to pay the casino for any losses. Because the junket operator is responsible for collecting from the patrons, casinos see little need to investigate the patron's ability to cover his/her potential debt or the source of his/her wealth.

Although there is a legal requirement to declare to Cambodian Customs the entry of more than U.S. $10,000 into the country, in practice there is no effective oversight of cash movement into or out of Cambodia. Article 13(1) of the Law of Foreign Exchange requires the import or export of any means of payment equal to or exceeding U.S. $10,000 or equivalent to be reported to the Customs authorities at the border crossing point and Customs should transmit this information on a monthly basis to the NBC. Outbound travelers are in practice not required to fill in a declaration form concerning the amount of currency or negotiable instruments they are carrying. There is no explicit power to stop or restrain transported funds and negotiable instruments to ascertain whether evidence of money laundering or terrorist financing exists. No specific provisions exist to sanction persons involved in cross border cash smuggling for money laundering or terrorist financing purposes or to seize the cash or instruments involved. Therefore, Cambodia does not at present have a system in place for effective monitoring cross border movement of cash and monetary instruments as required by international standards on AML/CTF.

In 1996, Cambodia criminalized money laundering related to narcotics trafficking through the Law on Drug Control. In 1999, the government also passed the Law on Banking and Financial Institutions. Together with the 2007 AML/CTF law, these laws provide an additional legal basis for the NBC to regulate the financial sector. The NBC also uses the authority of these laws to issue and enforce new regulations. The Draft Criminal Code, which is currently under consideration by the Council of Ministers, has provisions to criminalize money laundering in relation to proceeds from all serious crime.

The 2007 Law on Counter Terrorism criminalizes terrorist financing; and regulations on transactions suspected of financing terrorism are covered by the AML/CTF law. Under the 2007 Law on Counter Terrorism, the Minister of Justice may order the prosecutor to freeze property of a legal or natural person if that person is listed on the list of persons and entities belonging or associated with the Taliban and Al Qaida issued by the UNSCR 1267 committee or if he is a person who has committed a offence as defined in the law or a corresponding offence under the law of another state. The NBC circulates to financial institutions the list of individuals and entities included on the UNSCR 1267 Sanction Committee's consolidated list, and reviews the banks for compliance in maintaining this list and reporting any related activity. To date, there has not been an opportunity to monitor compliance of these new provisions. However, there have been no reports of designated terrorist financiers using the Cambodian banking sector. Should sanctioned individuals or entities be discovered using a financial institution in Cambodia, the NBC has the legal authority to freeze the assets until prosecution commences and a competent court has adjudicated the case. Penal sanctions for convictions of money laundering or financing terrorism include seizure of the assets to become state property.

In May 2008, the UN Counter-Terrorism Committee Executive Directorate (CTED) visited Cambodia and commended the GOC for the significant progress achieved in developing its AML/CTF regime but also noted remaining deficiencies. The CTED recommended that the CAFIU be further empowered to develop implementation and coordination procedures and undertake related training and public awareness campaigns. The CTED also recommended the development of procedures to ensure adequate AML/CTF measures, in particular for casino operations and real estate transactions.

Cambodia is a party to the UN Drug Convention, the UN Convention Against Transnational Organized Crime, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. In June 2004, Cambodia joined the Asia/Pacific Group on Money Laundering (APG), a Financial Action Task Force (FATF) style regional body.

The Government of Cambodia (GOC) should take steps enact the Draft Criminal Code as a matter of priority so as to adopt a money laundering offence for proceeds of all serious crime. In addition, the GOC should strengthen control over its porous borders as well as increase the capability of its nascent FIU. The GOC should issue additional decrees necessary to fully implement the AML/CTF law—particularly implementing provisions relating to designated nonfinancial businesses and professions mandating compliance with reporting requirements established in the AML/CTF law. Developing the capability of its law enforcement and judicial authorities to investigate, prosecute, and adjudicate financial crimes are necessities. Establishing a national coordination group, including all relevant agencies involved in AML/CTF issues should be considered a high priority for the GOC to ensure that its AML/CTF regime comports with international standards.

Canada

Money laundering in Canada is primarily associated with drug trafficking and financial crimes, particularly those related to fraud. According to the Canadian Security Intelligence Service (CSIS), criminals launder an estimated $5 to $17 billion each year. With $1.5 billion in trade crossing the border each day, the United States and Canadian governments share concerns about illicit cross-border movements of currency, particularly the proceeds of drug trafficking. Organized criminal groups involved in drug trafficking also remain a challenge. CSIS estimates that approximately 950 organized crime groups operate in Canada, with approximately 80 percent of all crime groups in Canada involved in the illicit drug trade.

The Government of Canada (GOC) enacted the Proceeds of Crime (Money Laundering) Act in 2000 to criminalize money laundering, facilitate the investigation and prosecution of money laundering, and create the financial intelligence unit (FIU), known as the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). The Proceeds of Crime (Money Laundering) Act was amended in

December 2001 to become the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). The law expands the list of predicate money laundering offenses to cover all indictable offenses, including terrorism and trafficking in persons.

The PCMLTFA created a mandatory reporting system for suspicious financial transactions, large cash transactions, large international electronic funds transfers, and suspected terrorist property. Failure to file a suspicious transaction report (STR) could result in up to five years' imprisonment, a fine of approximately $2 million, or both. The law protects those filing suspicious transaction reports from civil and criminal prosecution.

The PCMLTFA requires reporting of all cross-border movement, including through the mail system, of currency and monetary instruments totaling or exceeding C$10,000 (approximately $7931), to the Canadian Border Services Agency (CBSA). Failure to report cross-border movements of currency and monetary instruments could result in seizure of funds or penalties ranging from C$250 to C$5,000 (approximately $198 to $3966). The CBSA forwards cross-border and cash seizure reports to FINTRAC. The CBSA also provides evidence to the RCMP, which investigates and brings charges. From April 2007 through March 2008, CBSA seizures totaled C$40 million (approximately $31.72 million). In the same interval, CBSA executed 130 "Level IV" seizures, which occur when a CBSA officer suspects funds are proceeds of crime or linked to terrorist activities.

In December 2006, Parliament passed Bill C-25, amending the PCMLTFA. This legislation expands the coverage of Canada's anti-money laundering (AML) and counterterrorist financing (CTF) regime and applies to banks; credit unions; life insurance companies; trust and loan companies; brokers/dealers of securities; foreign exchange dealers; money services businesses; sellers and redeemers of money orders; accountants; real estate brokers; and casinos. In December 2008, lawyers, notaries (in Québec and British Columbia only) and dealers in precious metals and stones became subject to the PCMLTFA. However, lawyers in several provinces have successfully filed legal challenges to the applicability of the PCMLTFA to them based upon common law attorney-client privileges, so lawyers are not completely covered by the AML provisions.

Bill C-25 enhances client identification and record-keeping by requiring greater scrutiny of correspondent banking relationships; enhanced monitoring of politically exposed persons; expanded record keeping and due diligence requirements for real estate agents and brokers; mandatory risk assessments to mitigate high risk activities for money laundering and terrorist financing; originator information for outgoing international wire transfers; and information on the beneficial owners of corporations. The Bill mandates that FINTRAC create a national registry for money service businesses, and establish a system to render administrative monetary penalties for noncompliance effective December 2008. FINTRAC's administrative monetary penalties regime provides for fines of up to C$1,000 ($793) for a minor violation, up to C$10,000(approximately $7931) for a serious violation, and as much as C$500,000 ($396,445) for a very serious violation.

In February 2008, the Financial Action Task Force (FATF) adopted a mutual evaluation report (MER) of Canada. The report stated that although Canada has strengthened its overall AML/CTF regime, shortcomings still existed, including the scope and coverage of the AML/CTF requirements applicable to designated nonfinancial business and professions. The report also cited concern regarding FINTRAC's effectiveness communicating relevant information to law enforcement authorities. The mutual evaluation on-site assessment visit took place after the passage of Bill C-25, but before Canada could implement all related measures. In June 2008, Canada implemented the bill, resulting in a somewhat stronger comportment with international standards. As a result of the implementation of the bill, authorities introduced a risk-based approach, required new client identification and recordkeeping requirements for real estate agents and brokers, and established a national registry of money service businesses to ensure sector compliance and transparency. Bill C-25 also permits FINTRAC to include

additional information in the intelligence product that it can disclose to law enforcement and national security agencies.

While Canada's Office of the Superintendent of Financial Institutions (OSFI) and other federal and provincial regulatory agencies supervise institutions for safety and soundness, FINTRAC is the sole authority with the mandate to ensure compliance with the PCMLTFA and associated regulations. FINTRAC recently revised regulations and guidelines explaining the PCMLTFA and its requirements to incorporate the most recent implementation of Bill C-25 effective June 2008. The guidelines provide an overview of FINTRAC's mandate and responsibilities, and include background information about money laundering and terrorist financing. The guidelines also provide an outline of requirements for maintaining a compliance regime, record-keeping, client identification, and reporting transactions.

Operational since 2001, FINTRAC is an independent agency with regulatory and FIU functions. FINTRAC has a staff of approximately 320 employees that work as analysts, compliance officers, and information technology specialists. FINTRAC receives and analyzes reports from regulated entities as mandated by the PCMLTFA, and disseminates its findings—disclosures—to law enforcement and intelligence agencies. FINTRAC has access to other law enforcement and national security agencies databases through an MOU and, on a case-by-case basis, with other relevant agencies. FINTRAC requires an MOU in order to exchange information and has signed 53 MOUs with foreign counterparts. From April 2007 to the end of March 2008, Canada sent 62 case disclosures to partner FIUs.

FINTRAC received over 21 million reports from reporting entities between April 2007 and the end of March 2008. These reports included more than 50,000 STRs more than 5.5 million cash transaction reports, in excess of 50,000 cross-border reports, and more than 16 million electronic funds transfer reports (which includes funds that enter and exit the country). FINTRAC may only disclose information related to money laundering or terrorist financing offenses. FINTRAC produced a total of 210 case disclosures between 2007 and 2008. Of the 210 case disclosures, 171 were suspected money laundering, 29 were suspected terrorist activity, and 10 involved suspected money laundering, terrorist financing, and/or threats to the security of Canada.

FINTRAC's compliance program is risk-based and emphasizes awareness training, compliance examinations, disclosures to law enforcement of reporting entities' noncompliance, and minimizing the regulatory burden for obligated entities. FINTRAC has Memoranda of Understanding (MOUs) with Canadian national regulators, including OSFI and the Investment Dealers Association of Canada (IDA), as well as provincial regulators. These MOUs permit FINTRAC and the regulators to exchange compliance information. From April 2007 through the end of March 2008, FINTRAC conducted 277 examinations with national and provincial regulatory agencies conducing 257 examinations for their respective sectors. FINTRAC identified and disclosed five cases of noncompliance for further law enforcement investigation and prosecution. OSFI completed 13 AML on-site compliance examinations of financial institutions. The Department of Finance has established a public/private sector advisory committee and is now coordinating a National Risk Assessment. In May 2008, the OSFI held an information session on the risk-based approach.

Although all Canadian police forces can investigate money laundering and terrorist financing offenses, the Royal Canadian Mounted Police (RCMP), in particular its Integrated Proceeds of Crime Initiative (IPOC) Units, and the provincial law enforcement authorities in Ontario (the Ontario Provincial Police) and Québec (Sûreté du Québec) undertake virtually all money laundering and terrorist financing investigations. In 2007, the RCMP opened 73 money laundering cases, and opened seven in the first four months of 2008; most have not concluded. The RCMP also seized approximately $8.9 million and forfeited $283,000 in 2007. In the first half of 2008, RCMP seized approximately $484,000.

The attorney general of Canada (through public prosecution offices) and provincial attorney generals prosecute money laundering and terrorist financing cases. In 2007, authorities charged targets with 150 possession of proceeds of crime charges, three specifically for money laundering, and in the first four months of 2008 registered four such charges, none specific to money laundering. In 2007 prosecutors obtained five convictions of the original 150 and none in 2008.

The PCMLTFA enables Canadian authorities to identify, deter, disable, prosecute, convict, and punish terrorist groups. The PCMLTFA expands FINTRAC's mandate to include counterterrorist financing and allow disclosures to CSIS of information related to financial transactions relevant to threats against Canadian security. The GOC also designates suspected terrorists and terrorist organizations on the UN 1267 Sanctions Committee's consolidated list. Financial institutions must freeze the assets of those designated. The PCMLTFA also prohibits fundraising for these organizations. There are currently more than 500 individuals and entities associated with terrorist activities designated by the GOC. Investigations indicate that terrorist cells generate funds locally through drug trafficking and various fraud schemes, and terrorist groups employ identical methods to money launderers including bulk cash smuggling; the use of the formal banking sector; money exchange/transfer services; and emerging technology such as internet transfer systems. To deter the exploitation of nonprofit and charitable organizations by terrorists, the 2001 reforms criminalize knowingly collecting or providing funds to carry out terrorism. They also denied or removed special charitable status from nonprofits supporting terrorism; and facilitated freezing and seizing their assets.

Canada has longstanding agreements with the U. S. on law enforcement cooperation, including treaties on extradition and mutual legal assistance, as well as an asset sharing agreement. Recent cooperation concerns focus on the inability of U.S. and Canadian law enforcement officers to exchange information promptly concerning suspicious sums of money found in the possession of individuals attempting to cross the United States-Canadian border. A 2005 MOU between the CBSA and the U.S. Department of Homeland Security's Immigration and Customs Enforcement (ICE) on exchange of cross-border currency declarations expanded the extremely narrow disclosure policy. However, the scope of the exchange remains restrictive. To remedy this, the CBSA is developing an information-sharing MOU with the United States related to its Cross-Border Currency Reporting Program.

Canada is a party to the UN Convention for the Suppression of the Financing of Terrorism, the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption.

Canada is a member of the FATF as well as the Asia/Pacific Group on Money Laundering (APG), and is a supporting nation of the Caribbean Financial Action Task Force (CFATF). Canada also belongs to the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. FINTRAC is a member of the Egmont Group, which maintains its Secretariat in Toronto. The GOC is contributing approximately $5 million over a five-year period to help establish the Secretariat.

The Government of Canada has demonstrated a strong commitment to combat money laundering and terrorist financing both domestically and internationally. In 2008, the GOC continued to make strides in enhancing its AML/CTF regime, and reducing its vulnerability to money laundering and terrorist financing. The GOC should continue to ensure that its privacy laws do not excessively prohibit provision of information to domestic and foreign law enforcement that might lead to prosecutions and convictions. FINTRAC should maintain its new registry of money services bureaus, making use of the registry and executing compliance examinations. The GOC should also continue to improve the communication between FINTRAC and law enforcement authorities. The GOC should ensure effective reporting of cross-border reports to FINTRAC and increase efforts to share information in this regard with U.S. counterparts.

Cayman Islands

The Cayman Islands, a United Kingdom (UK) Caribbean overseas territory, continues to make strides in strengthening its anti-money laundering and counterterrorist financing regime. However, the islands remain vulnerable to money laundering due to their significant offshore sector. Most money laundering that occurs in the Cayman Islands is primarily related to fraud and drug trafficking. Due to their status as a zero tax regime, the Cayman Islands is also considered attractive to those seeking to evade taxes in their home jurisdiction.

The Cayman Islands is home to a well-developed offshore financial center that provides a wide range of services, including banking, structured finance, and investment funds, various types of trusts, and company formation and management. As of December 2008, there are approximately 278 banks, 159 active trust licenses, 773 captive insurance companies, seven money service businesses, and more than 62,572 exempt companies licensed or registered in the Cayman Islands. At the end of June 2008, there were 10,037 hedge funds registered, up from 9,413 at the end of 2007, according to the Cayman Islands Monetary Authority (CIMA). Shell banks are prohibited, as are anonymous accounts. Bearer shares can only be issued by exempt companies and must be immobilized. Gambling is illegal; and the Cayman Islands does not permit the registration of offshore gaming entities. As an offshore financial center with no direct taxes and a strong reputation for having a stable legal and financial services infrastructure, the Cayman Islands is attractive to businesses based in the United States and elsewhere for legal purposes but also equally attractive to criminal organizations seeking to disguise the proceeds of illicit activity.

The Misuse of Drugs Law and the Proceeds of Criminal Conduct Law (PCCL) criminalize money laundering related to narcotics trafficking and all other serious crimes.

The Proceeds of Crime Law 2008 (POCL) came into effect in September 2008. The law repeals and replaces the Proceeds of Criminal Conduct Law (2007 revision). The POCL introduces the concept of criminal property (includes terrorist property) that constitutes a person's benefit (directly or indirectly) from criminal conduct; tax offenses are not included. No longer applicable to an indictable offense, the term criminal conduct was also amended to cover any offense. Extraterritorial and appropriate ancillary offenses are covered in domestic legislation and criminal liability extends to legal persons. The POCL also consolidates the law relating to the confiscation of the proceeds of crime and the law relating to mutual legal assistance in criminal matters. The penalties for money laundering are $5000 Cayman Island (KYD) dollars (approximately $6,125) fine and/or imprisonment for two years for summary conviction, and a fine and/or imprisonment for 14 years on conviction on indictment.

The Cayman Islands Monetary Authority (CIMA) is responsible for the licensing, regulation and supervision of the Cayman Islands' financial industry, as well as monitoring the industry for compliance with its anti-money laundering and counterterrorist financing (AML/CTF) obligations. The financial industry includes banks, trust companies, investment funds, fund administrators, insurance companies, insurance managers, money service businesses, and corporate service providers. These institutions, as well as most designated nonfinancial businesses and professions, are subject to the AML/CTF regulations set forth in the Money Laundering (Amendment) Regulations 2008, which came into force on October 24, 2008. A 2007 amendment to the Money Laundering Regulations brought dealers of precious metals and stones under the definition of relevant financial businesses, and they were given a transitional grace period until January 1, 2008 for compliance. The real estate industry is also subject to AML/CTF regulations, but the CIMA does not have responsibility for supervising this sector.

Guidance Notes on the Prevention and Detection of Money Laundering and Terrorist Financing (Guidance Notes) are issued by the CIMA and were last amended in December 2008. The amendments, among other things, require institutions to keep appropriate evidence of client identification, account opening or new business documentation. Adequate records identifying relevant

financial transactions should be kept for a period of five years following the closing of an account, the end of the transaction or the termination of the business relationship. This includes records pertaining to inquiries about complex, unusual large transactions, and unusual patterns of transactions. The amendments also address correspondent banking and enhanced due diligence procedures. Financial institutions are prohibited from correspondent relationships with shell banks. In addition, financial institutions must satisfy that respondent financial institutions in a foreign country do not permit their accounts to be used by shell banks.

The CIMA conducts on-site and off-site examinations of licensees. These examinations include monitoring for compliance with the POCL and the CIMA's Guidance Notes. Additional requirements of the Guidance Notes require employee training, record keeping, and "know your customer" (KYC) identification requirements for financial institutions and certain financial services providers. The regulations require due diligence measures for individuals who establish a new business relationship, engage in one-time transactions over KYD $15,000 (approximately $18,000), or who may be engaging in money laundering. The application of the AML/CTF measures to the financial sector and designated nonfinancial businesses is not based on risk assessment, although the CIMA does employ a risk-based approach to its on-site inspections.

The PCCL requires mandatory reporting of suspicious transactions, and makes failure to report a suspicious transaction a criminal offense that could result in fines or imprisonment. A suspicious activity report (SAR) must be reported once it is known or suspected that a transaction may be related to money laundering or terrorist financing. There is no threshold amount for the reporting of suspicious activity. Tipping off provisions were broadened through the POCL and include situations where an individual knows or suspects that criminal conduct is about to take, is presently taking, or has taken place. The penalties for tipping off were increased to a KYD $5000 fine and/or imprisonment for two years for summary conviction, and a fine and/or imprisonment for five years on conviction on indictment.

Established under PCCL (Amendment) Law 2003, the Financial Reporting Authority (FRA) replaces the former financial intelligence unit of the Cayman Islands. The FRA is responsible for, among other things, receiving, analyzing, and disseminating SARs, including those relating to the financing of terrorism. The FRA began operations in 2004 and has a staff of six: a director, a legal advisor, a senior accountant, a senior analyst, a junior analyst, and an administrative officer. The FRA is a separate civilian authority governed by the Anti-Money Laundering Steering Group (AMLSG), which is chaired by the Attorney General and includes as its members the Financial Secretary, the Managing Director of the Cayman Islands Monetary Authority, the Commissioner of Police, the Solicitor General, and the Collector of Customs. Obligated entities currently report suspicious activities to the FRA via fax, although the FRA plans to establish an electronic reporting system. From June 2007 through June 2008, the FRA reviewed 247 cases and made 70 disclosures to domestic and foreign law enforcement and regulatory agencies. The majority of reports filed were related to suspicious financial activity, fraud, and money laundering. Under the PCCL, the FRA has the authority to require all obligated entities to provide additional information related to a SAR. The FRA can request a court order to freeze bank accounts if it suspects the account is linked to money laundering or terrorist financing. The FRA is an active member of the Egmont Group and has Memoranda of Understanding in place with Australia, Canada, Chile, Guatemala, Indonesia, Mauritius, Nigeria, Thailand, and the United States.

The Financial Crime Unit (FCU) of the Royal Cayman Islands Police Service (RCIP) is responsible for investigating money laundering and terrorist financing. The FCU works in conjunction with the Joint Intelligence Unit (JIU), which gathers and disseminates intelligence to domestic and international law enforcement agencies. The Legal Department of the Portfolio of Legal Affairs is responsible for prosecuting financial crimes. In July 2008, the FCU arrested an individual in connection with the collapse of the Grand Island Fund following serious irregularities in the fund's

trading activities. The collapse of the fund is believed to involve millions of dollars. The FCU investigation is ongoing.

On August 10, 2007, the Cayman Islands enacted the Customs (Money Declarations and Disclosures) Regulations, 2007. These regulations establish a mandatory declaration system for the inbound cross-border movement of cash and a disclosure system for money that is outbound. All persons transporting money totaling KYD $15,000 (approximately $18,000) or more into the Cayman Islands are required to declare such amount in writing to a Customs officer at the time of entry. Persons carrying money out of the Cayman Islands are required to make a declaration upon verbal or written inquiry by a Customs officer.

The Cayman Islands has a comprehensive system in place for the confiscation, freezing, and seizure of criminal assets. In addition to criminal forfeiture, civil forfeiture is allowed in limited circumstances. The POCL provides the Attorney-General with the ability to issue restraint orders once an investigation has begun without the need to bring charges within 21 days. Confiscation orders may also now be made by the Attorney-General upon conviction in either Summary or Grand Courts. The legislation also permits the Attorney General to bring civil proceedings for the recovery of the proceeds of crime. Over $120 million in assets has been frozen or confiscated since 2003.

The Cayman Islands is subject to the United Kingdom Terrorism (United Nations Measure) (Overseas Territories) Order 2001 (TUNMOTO). The Cayman Islands criminalized terrorist financing through the passage of the Terrorism Bill 2003, which extends criminal liability to the use of money or property for the purposes of terrorism. It also contains a specific provision on money laundering related to terrorist financing. While lists promulgated by the UN Sanctions Committee and other competent authorities are legally recognized, there is no legislative basis for independent domestic listing and delisting. The confiscation, freezing, and seizure of assets related to terrorist financing are permitted by law. Nonprofit organizations must be licensed and registered, although there is no competent authority responsible for their supervision. There have been no terrorist financing investigations or prosecutions to date in the Cayman Islands.

In 1986, the United States and the United Kingdom signed a Treaty concerning the Cayman Islands relating to Mutual Legal Assistance (MLAT) in Criminal Matters. By a 1994 exchange of notes, Article 16 of that treaty has been deemed to authorize asset sharing between the United States and the Cayman Islands. Many U.S. investigations involve, at some stage, a defendant who has secreted funds in the Caymans, often in accounts held by offshore trust entities. Although generally helpful when receiving formal MLAT requests from the U.S. for assistance, the Cayman Islands has not been proactive with regard to money laundering prosecutions based on its own investigations.

The Cayman Islands is a member of the Caribbean Financial Action Task Force (CFATF), a FATF-style regional body. In November 2007, CFATF conducted its third mutual evaluation of the Cayman Islands. The evaluation found the Cayman Islands to be compliant or largely compliant with 38 of the Forty-Nine Financial Action Task Force recommendations and noted that a strong culture of compliance exists within the AML/CTF regime. However, recommendations to address remaining weaknesses were identified. Over the course of 2008, the Cayman Islands revised legislation in accordance with most of the recommendations made in the report including the following: The Proceeds of Crime Law (POCL) was enacted in June 2008; The Money Laundering (Amendment) Regulations 2008 became enforceable in October 2008; The Guidance Notes on the Prevention and Detection of Money Laundering and Terrorist Financing (GN) was revised and issued in September 2008.

In March 2008, the United Kingdom published The Foreign and Commonwealth Office: Managing Risk in the Overseas Territories. In terms of AML/CTF, the Foreign and Commonwealth Office indicated that regulatory standards in most Territories are not up to those of the Crown Dependencies (Jersey, Guernsey and the Isle of Man) and that a lack of capacity has reduced the ability of Territories

to investigate and prosecute money laundering. However, the report noted that only the Cayman Islands has, so far achieved successful prosecutions of local participants for offshore money laundering offenses. This trend will hopefully continue in the future, as it sets a model for other offshore financial sectors in the Caribbean basin. There have been only five money laundering convictions in the Cayman Islands since 2003, which is not a large amount considering the size of the Caymans' financial sector and the volume of offshore entities holding assets there.

In July 2008, the U.S. Government Accountability Office (GAO) issued a report entitled: "Cayman Islands: Business and Tax Advantages Attract U.S. Persons and Enforcement Challenges Exist." The report was conducted in response to a Congressional inquiry regarding offshore tax evasion; the business activities of U.S. taxpayers involving a corporate service provider in the Cayman Islands; the extent, motives, and tax implications of these activities; and the extent that the U.S. government has examined these activities.

The report found that U.S. persons who conduct financial activity in the Cayman Islands commonly do so to gain business advantages, such as facilitating U.S.-foreign transactions or to minimize or obtain tax advantages; while much of this activity is legal, some is not. In June 2008, two former Bear Stearns hedge fund managers were arrested and indicted in the U.S. on conspiracy and fraud charges related to the collapse of two Cayman Islands funds they oversaw. A companion civil suit to recover over $1.5 billion in losses was filed against four individuals and companies in the Cayman Islands. The report did highlight the cooperation between U.S. agencies and its Cayman counterparts in investigating money laundering, financial crimes, and tax evasion. In general, U.S. officials said that cooperation with its Cayman counterparts has been good and that compliance problems are not more prevalent than elsewhere offshore.

The Government of the Cayman Islands bolstered its AML/CTF regime in 2008, to be in accordance with international standards. However, for a jurisdiction with one of the largest and most developed offshore sectors, the Cayman Islands should continue to strengthen and implement its AM.L/CTF regime to include ensuring the new provisions related to AML/CTF requirements for dealers in precious metals and stones. Additionally, the disclosure/declaration system for the cross-border movement of currency should be fully implemented. The Cayman Islands also should work to fully develop its capacity to investigate and prosecute money laundering and terrorist financing cases.

Chile

Chile has a large and well-developed banking and financial sector. Systemic vulnerabilities in Chile's anti-money laundering and combating the financing of terrorism (AML/CTF) regime include stringent bank secrecy laws that emphasize privacy rights impede Chilean efforts to identify and investigate money laundering and terrorist financing, as well as relatively new regulatory institutions in which oversight gaps remain. The Government of Chile (GOC) is actively seeking to turn Chile into a global financial center, but not an offshore financial center. Chile has Free Trade Agreements with 55 countries and is negotiating four more. Increased trade and currency flows, combined with an expanding economy, could attract illicit financial activity and money laundering. Given Chile's extensive trading partnerships and long and somewhat porous borders, its largely unregulated free trade zones are additional vulnerabilities. Illicit proceeds from limited drug trafficking and domestic consumption are laundered in the country.

Chile criminalized money laundering under Law 19.366 of 1995, Law 19.913 of 2003, and Law 20.119 of 2006. Law 19.913 identifies predicate offenses for money laundering, which include narcotics trafficking, terrorism in any form and the financing of terrorist acts or groups, illegal arms trafficking, kidnapping, fraud, corruption, child prostitution, pornography, and some instances of adult prostitution. Chile has yet to widen the scope of money laundering to apply it to other types of crimes such as trafficking in persons, intellectual property rights violations, and extortion.

Chile's financial intelligence unit (FIU) is the Unidad de Análisis Financiero (UAF), created by Law 19.913. The UAF is an autonomous agency affiliated with the Ministry of Finance and has a staff of 32—an increase from 21 personnel in 2007. It does not have criminal investigative or regulatory responsibilities. Law 19.913 requires mandatory reporting of suspicious transactions to the UAF, but does not establish specific parameters to determine irregular or suspicious activity. The UAF may access any government information (police, taxes, etc.) not covered by secrecy or privacy laws. The UAF can issue general instructions, such as requiring obligated entities to report any transactions by persons suspected of terrorist financing.

Financial institutions subject to suspicious transaction reporting requirements include banks, savings and loan associations, financial leasing companies, general and investment funds-managing companies, pension fund administration companies, the Foreign Investment Committee, money exchange firms and other entities authorized to receive foreign currencies, firms that carry out factoring operations, credit card issuers and operators, securities companies, money transfer and transportation companies, stock exchanges, stock exchange brokers, securities agents, insurance companies, mutual funds managing companies, forwards and options markets operators, tax-free zones' legal representatives, casinos, gambling houses and horse tracks, customs general agents, auction houses, realtors and companies engaged in the land development business, notaries and registrars, and sports clubs. Dealers in jewels and precious metals, and intermediaries (such as lawyers and accountants) are not subject to reporting requirements.

In addition to filing suspicious transaction reports (STRs), Law 19.913 also requires that obligated entities maintain registries of cash transactions that exceed 450 unidades de fomento (UF) (450 UF is approximately $15,000). All cash transaction reports (CTRs) contained in the internal registries must be sent to the UAF at least once a year, or more frequently at the request of the UAF. The UAF requires banks to submit CTRs every month, and money exchange houses and most other obliged institutions every three months. Some specific institutions without a high amount of cash transactions (e.g. notaries) may submit CTRs every six months. In all cases, institutions must report CTRs dating from May 2004, when the obligation to record cash transactions over 450 UF went into effect. The UAF had received 1,312 CTRs through June 2008, and 311 STRs through September 2008.

The physical transportation of cash exceeding $10,000 into or out of Chile must be reported to Customs, which then files a report with the UAF. These reports are sent to the UAF daily. However, Customs and other law enforcement agencies are not legally empowered to seize or otherwise stop the movement of funds, and the GOC does not impose a significant penalty for failing to declare the transportation of currency in excess of the threshold amount. Since the beginning of 2008, a new pilot system that allows for better management of information by the UAF was put in place. The system allows Customs to file its reports directly from the place where the activity being reported is taking place. At this point, the system is fully operational at the Santiago Airport's Customs and in the process of being implemented in the rest of the country.

Law 20.119 authorizes the UAF to impose sanctions on obligated entities if they fail to comply with requirements to establish an AML/CTF system or report suspicious cash transactions. The sanctions range from warning letters to fines. In 2008, the UAF identified 35 cases where entities failed to comply with ALM/CTF requirements or report suspicious cash transactions. The UAF levied fines in 29 of the 35 cases. Of these 35 cases, nine involved factoring companies and eight involved currency exchange houses.

The UAF continues to develop its capabilities. In 2008, it created a compliance division to ensure that required entities meet reporting requirements. The compliance division will initially focus on currency exchange houses. The Association of Banks and Financial Institutions, the Superintendence of Banks and Financial Institutions (SBIF), and the UAF provide training and resources to required reporting entities. In 2008, the UAF organized several money laundering seminars for compliance officers at

banks and currency exchange houses. The UAF also issued instructions to customs agents and real estate agents that emphasized the importance of "know your customer" (KYC) requirements.

The SBIF supervises and regulates banks in Chile. Stock brokerages, securities firms, and insurance companies are under the supervision and regulation of the Superintendence of Capital Markets. Chile's anti-money laundering laws oblige banks to abide by KYC standards and other money laundering controls for checking accounts. The same compliance standards do not apply to savings accounts. Only a limited number of banks rigorously apply money laundering controls to noncurrent accounts. Banks and financial institutions must keep records with updated background information on their clients throughout the period of their commercial relationship, and maintain records for a minimum of five years on any case reported to the UAF.

Chile's gaming industry is supervised by the Superintendence of Casinos (SCJ). The SCJ is responsible for drafting regulations about casino facilities and managing the development of the industry. Online gambling is prohibited except for the Internet purchase of lottery tickets from one of Chile's two lotteries. Sixteen casinos are currently operating throughout the country. The SCJ has oversight powers and regulatory authority over the industry but no law enforcement authority. Under Law 19.995, the SCJ granted authorization for 15 new casinos to operate in Chile after participating in an international and domestic bidding process to assign permits during 2005 and 2006. Eight new casinos opened in 2008. Six more are expected to open in 2009, bringing the total number of casinos to 22. The SCJ screened applications for the new casino licenses with the support of domestic and international police and financial institutions. Chilean law, however, limited the SCJ to 270 days for the entire background check and determination of whether to issue a license.

Law 19.913 requires casinos to keep a record of all cash transactions over UF 450 (approximately $15,000) and to designate a compliance officer. According to the GOC, the UAF issued a regulation jointly with the SCJ, which verifies that to date 100 percent of operational casinos have: a compliance officer; an AML/CTF manual; and on site supervision and enforcement. In addition, the UAF instructed casinos to identify, know, and maintain records on all customers—Chileans and foreigners—who carry out any cash transaction over $3,000; this is a reduction in the cash transaction threshold from $10,000. The SCJ also requires the casinos to prepare and submit for approval manuals detailing their AML/CTF plan The SCJ is actively working to establish additional regulations, internal control standards, and standardized forms to improve their ability to monitor the growing number of casinos. Chile's Finance Ministry, in cooperation with the SCJ, presented to Congress a draft law addressing some of the weaknesses of Chile's gaming law. The draft law, if it passes, will provide increased regulatory authority to the SJC and prohibit individuals without licenses from operating electronic gambling games.

While the regulatory and oversight system established by Chile for banks, financial institutions, and the gaming industry provides a foundation to combat money laundering, there are weaknesses. For example, there is no common definition for "suspicious activity" among financial institutions. The UAF publishes a list of warning signs to help reporting entities identify suspicious activity, but financial institutions are given wide latitude to police themselves regarding activities that could be considered suspicious. Another weakness is the absence of regulatory oversight for nonbank financial institutions such as money exchange houses and cash couriers. There are more than 60 money exchange houses in Santiago and 125 registered with the UAF throughout the country. While money exchange houses must register with the UAF, they are not supervised by any regulatory body. Non-bank financial institutions must obtain contact information and a declaration of origin statement from individuals carrying out transactions of more than $5,000. These institutions must also report transactions of up to $4,999 to the UAF if they are considered to be suspicious. This sector appears particularly vulnerable to abuse by money launderers.

The Public Ministry directs the investigation and prosecution of money laundering cases. When the UAF receives a STR or a CTR, it analyzes the information and determines if an account or a case requires further investigation. If a case requires further investigation, the UAF passes the information to the Public Ministry. The Public Ministry is responsible for receiving and investigating all cases from the UAF and has up to two years to complete an investigation and begin prosecution. Through September, the UAF referred 47 cases to the Public Ministry.

The Public Ministry's unit for money laundering and economic crimes proactively investigates potential crimes and seeks opportunities to enhance its capabilities. Public prosecutors in all regions have received training on money laundering. The money laundering unit has also developed reference materials for prosecutors, including a manual that provides practical steps to investigate assets in order to identify possible money laundering as well as drug trafficking. They have also established a computer link with the tax service, SBIF, and other relevant agencies to access information that is not protected by bank and tax secrecy laws.

The Chilean investigative police (PDI) and the uniformed national police (Carabineros) work in conjunction with the Public Ministry on money laundering investigations. The PDI has an economic crimes division and a unit dedicated to money laundering investigations. They also cooperate with U.S. and regional law enforcement in money laundering investigations. In 2004, this cooperation resulted in the break-up of an international money laundering ring that involved smugglers in Colombia, Chile and the United States.

The Public Ministry and police are competent and professional, but there are several factors that limit their ability to successfully investigate and prosecute money laundering cases. The units in charge of money laundering investigations and prosecutions are new and do not have extensive experience. There is a shortage of qualified investigators to pursue cases, and some institutional resistance to the idea that money laundering is worth prosecuting. Regulations also restrict information sharing among different agencies. Under the current money laundering laws, the UAF is prohibited from giving information directly to the PDI or Carabineros. The UAF is only permitted to share information with the Public Ministry and foreign FIUs. The PDI or Carabineros must request financial information from the Public Ministry, which in turn requests it from the UAF. The UAF responds with all available information, which the Public Ministry gives to the PDI or Carabineros, but this process costs valuable time.

The most significant obstacle to money laundering investigations is bank secrecy. Article 154 of the General Banking Law places all types of bank deposits and obligations under banking secrecy, and only allows banking institutions to share information about such transactions with the depositor or creditor (or an authorized legal representative). Law 707 states that banks may not share information about the movement and balances in a current account with a third party. Due to these legal restrictions, banks do not share information with prosecutors without a judicial order. Some banks and their compliance officers aggressively apply rigorous, international AML/CTF standards, but they are restricted to simply reporting suspicious activity and then waiting for the appropriate court authorization to release any private information. Other banks are slow to reply to judicial court orders to provide prosecutors with additional information. Police and prosecutors complain they lose valuable time waiting at least a month (but usually more) for some banks to provide information. Judges can require the detention of the bank's general manager until all information is disclosed, but this tool is rarely used. In the instances when the judge has issued the order for the general manager's detention, bank information was provided immediately.

Under Law 20.119, the Public Ministry can, with the authorization of a judge, lift bank secrecy provisions to gain account information if the account is directly related to an ongoing case. Unless a STR has been filed on an account, prosecutors and the UAF must get permission from a judge to examine an account. The process is often subject to the determination of judges who have received

little training in financial crimes. The judges must decide if the prosecutors have presented sufficient evidence to warrant lifting bank secrecy. This process often prohibits prosecutors and the UAF from accessing the information they would need to convince a judge of suspicious activity. The UAF has always received permission to examine an account when requested, but it has only made requests when it was confident the judge would comply. The system does not encourage aggressive examination of suspicious activity on the part of the UAF, and time is lost in the preparation of the case for the judge.

A draft law under review in a committee of Chile's House of Representatives would facilitate easier access to bank and tax records for the UAF and prosecutors in certain instances. If passed, this law would bring Chile into greater compliance with the Financial Action Task Force (FATF) recommendations, and UN resolutions on terrorist financing. The draft law has been sitting in the Congressional commission since it was introduced in May 2007. The Organization for Economic Cooperation and Development (OECD), to which Chile hopes to accede, criticized Chile's bank secrecy laws in October 2007. Chile's Foreign Minister used the opportunity to encourage passage of the draft law.

Law 19.913 contains provisions that allow prosecutors to request that assets be frozen only when tied to drug trafficking. No provisions have been made for freezing assets under other circumstances, including assets of individuals or companies designated by UN Security Council Resolution 1267. The Ministry of National Property currently oversees forfeited assets. Proceeds from the sale of forfeited assets are passed directly to CONACE, the National Drug Control Commission, to fund drug abuse prevention and rehabilitation programs. Under the present law, forfeiture is possible for real property and financial assets. Chilean law does not permit the seizure of substitute assets or civil forfeiture. The same draft law that would facilitate lifting bank secrecy for the UAF and Public Ministry would also allow for the freezing of assets in cases of suspected terrorist financing and would enable Chile to share seized assets with other governments. The draft law would also ensure assets seized in money laundering convictions would go, at least in part, to law enforcement rather than only to drug rehabilitation programs. The GOC seized just over $2 million in assets in 2008.

The GOC pursued 14 money laundering cases in 2008. Eleven cases were tied to drug trafficking, two of which were by-products of public corruption cases, and one derived from a prostitution case. The public corruption and prostitution cases are the first money laundering cases to be prosecuted that are not tied to drug trafficking. One case has led to a conviction and the other 13 cases are awaiting trial. The majority of the accused are being held in pre-trial detention. In the case that led to a conviction, the prosecution charged a Chilean member of an international criminal organization with drug trafficking and money laundering. The criminal organization included members from Mexico and Colombia. The defendant concealed illicit proceeds from drug sales and invested the money in various businesses. The defendant was sentenced to 10 years in prison; the case is noteworthy because of its complexity and international connections. While the GOC pursued two money laundering cases tied to public corruption in 2008, public corruption does not contribute significantly to money laundering in Chile. There is no indication that financial institutions engage in currency transactions involving international narcotics proceeds from significant amounts of U.S. currency or currency derived from drug sales in the United States. Most money laundering cases have been connected to domestic drug dealing. Detection methods, particularly when not tied to drug trafficking, are still weak. It is difficult to determine if other crimes, such as smuggling of goods, are connected to money laundering or if trade-based money laundering occurs. Given Chile's extensive trading partnerships, long borders, and advanced financial system, it is possible that criminal organizations, in addition to drug smugglers, use Chile as a money laundering location.

Chile has free trade zones in Iquique and Punta Arenas. The Iquique free trade zone is the larger of the two and has over 1,600 companies conducting retail and wholesale operations. It is located in northern Chile and has an extension in Arica, near Chile's border with Peru. Punta Arenas is located in southern

Chile and is relatively small compared to Iquique. The physical borders of both free trade zones are porous and largely uncontrolled. All companies in the free trade zones are reporting entities and are required to report any suspicious activity to the UAF. It is nearly impossible to determine the extent of money laundering in the free trade zones. Detection methods are weak and Chilean resources to combat the issue are limited. Iquique is the primary conduit for counterfeit goods into Chile, and one of the main conduits of counterfeit goods moving to the Tri-Border Area between Brazil, Paraguay, and Argentina. Police investigative efforts suggest possible criminal links between Iquique and the Tri-Border Area involving both terrorist financing of Hezbollah and Hamas and money laundering.

Laws 18.314 and 19.906 criminalize terrorist financing in Chile. Law 19.906 modifies Law 18.314 to more efficiently sanction terrorist financing in conformity with the UN International Convention for the Suppression of the Financing of Terrorism. Under Law 19.906, financing a terrorist act and the provision, directly or indirectly, of funds to a terrorist organization are punishable by five to ten years in prison. The SBIF circulates the UNSCR 1267 Sanctions Committee's consolidated list to banks and financial institutions. The UAF also posts the 1267 list on its website and has instructed all reporting entities to report any transactions by those on the list. To date, the GOC has not identified any terrorist assets belonging to individuals or groups named on the list. Law enforcement lacks tools to investigate terrorist financing; undercover operations, for example, are not permitted for such investigations

The GOC does not monitor transactions outside of Chile to prevent terrorist financing, nor does it regulate nongovernmental organizations (NGOs). Nonprofit organizations must register at the Justice Ministry, but this Ministry has no regulatory responsibility over them. In response to the evaluation of Chile by GAFISUD, which was released in December 2006, the Finance Ministry initiated discussions with the SBIF and the Superintendence of Capital Markets to identify the best way to monitor NGOs; these discussions have not yet reached conclusions.

Chile is party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. Chile is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and GAFISUD. During the GAFISUD Plenary XIV, Chile's Mutual Evaluation Report was approved. According to the GAFISUD procedures, the report was approved and a process of "intensive monitoring" was established. This was a result of low ratings on compliance with key FATF Recommendations. In the case of Chile, the evaluators rated Chile "partially compliant" on FATF Recommendation 5, which relates to customer due diligence and record keeping, and rated Chile "not compliant" on FATF Special Recommendation IV, which centers on reporting of terrorist-related suspicious transactions. The UAF is a member of the Egmont Group of FIUs and serves as one of the representatives for the Americas on the Egmont Committee. The UAF has signed memoranda of understanding (MOUs) for the exchange of financial information with the United States FIU and FIUs of 32 other jurisdictions

The GOC is proactive in pursing partnerships with other countries. It signed an agreement with Colombia in 2007 to cooperate on terrorism and economic crimes. There is no regular, formal exchange of records with the United States, but case-specific cooperation and exchange of records occurs, including the exchange of sensitive financial information with Financial Crimes Enforcement Network (FinCEN), the UAF's counterpart in the United States, through the Egmont Secure Web. The U.S. Government (USG) and GOC continue their judicial and investigative cooperation via the Inter-American Convention on Mutual Assistance in Criminal Matters. In 2008, the Carabineros joined the U.S. Federal Bureau of Investigation's (FBI) South American Fingerprint Exchange project that allows Chile and the USG to share fingerprint records of criminals. In addition, the FBI signed Memorandum of Cooperation agreements with the Carabineros, PDI, the Public Ministry, and the Customs agency for increased cooperation on transnational criminal investigations. As a result, there has been a significant increase in the amount of interaction and information exchange between the USG and GOC. As part of Chile's strategy to access the OECD, Chile participates, as an observer or

invitee, in 18 OECD Committees and Working Groups, including the Working Group on Bribery and Transnational Crimes.

Chile's anti-money laundering efforts continue to mature. The investigation and prosecution of three money laundering cases that are not tied to drug trafficking is an important step for the GOC. At the same time, the GOC can still do more to investigate complex money laundering schemes, such as trade-based money laundering. The UAF and the Public Ministry signed a collaboration agreement in October 2008 that aims to improve communication and cooperation between organizations. Given the current legal structure that separates reporting suspicious activity from investigating and prosecuting suspicious activity, it is essential that these institutions establish procedures to quickly and effectively share information and resources. The GOC should also expand the list of predicate crimes for money laundering to include all serious crimes, such as trafficking in persons and intellectual property rights violations, as well as establish regulatory control over nonbank institutions such as money exchange houses and charities. The GOC should ensure the passage of the draft law currently pending in the lower house of Congress to allow for the lifting of bank secrecy and the freezing of assets. Passage of this law would bring Chile closer to compliance with its UNSCR 1267 obligations and FATF Recommendations. The GOC should also increase government oversight of nonfinancial institutions, allow for greater access to information for the UAF and other key agencies, and enhance inter-agency cooperation to improve Chile's ability to combat money laundering and terrorist financing.

China, People's Republic of

Over the past five years, the Government of the People's Republic of China has made significant progress in developing anti-money laundering (AML) and counterterrorist financing (CTF) measures including legislative reform, strengthening enforcement mechanisms, and implementing international cooperation initiatives. However, money laundering remains a serious concern as China restructures its economy and develops its financial system. Narcotics trafficking, smuggling, trafficking in persons, counterfeiting of trade goods, fraud, tax evasion, corruption, and other financial crimes are major sources of laundered funds. Most money laundering cases currently under investigation involve funds obtained from corruption and bribery. Proceeds of tax evasion, recycled through offshore companies, often return to China disguised as foreign investment and, as such, receive tax benefits. Chinese officials have noted that most acts of corruption in China are closely related to economic activities that accompany illegal money transfers. Observers register increasing concern regarding underground banking and trade-based money laundering.

The People's Bank of China (PBOC), China's central bank, maintains primary authority for AML/CTF coordination. The PBOC shares some AML responsibilities with other financial regulatory agencies, including: the China Banking Regulatory Commission (CBRC), which supervises and regulates banks, asset management companies, trust and investment companies, and other deposit-taking institutions; the China Insurance Regulatory Commission (CIRC), which supervises the insurance sector; and the China Securities Regulatory Commission (CSRC), which supervises the securities sector. The Ministry of Public Security (MPS) has both an Anti-Money Laundering (AML) Division and an Anti-Terrorism Bureau, which lead anti-money laundering and counterterrorist finance-related law enforcement efforts.

China has criminalized money laundering under three separate articles of the Penal Code. China introduced Article 349 of the Penal Code in December 1990 to criminalize the laundering of proceeds generated from drug-related offenses, and amended Articles 191 and 312 of the Penal Code in June 2006. Article 191 expands the criminalization of money laundering to additional categories of predicate offences: narcotics trafficking, smuggling, organized crime, terrorism, embezzlement and bribery, financial fraud and disrupting the financial management order. The Article 191 amendments to seven predicate offenses, including fraud, bribery, and embezzlement, narcotics trafficking,

organized crime, smuggling, and terrorism. Article 312 criminalizes money laundering on the basis of an all-crimes approach, and criminalizes complicity in concealing the proceeds of criminal activity. The Financial Action Task Force (FATF) 2007 mutual evaluation report (MER) identified several deficiencies in China's criminalization of money laundering. These included the failure to fully cover the sole and knowing acquisition and use; criminalize self-laundering; provide for corporate criminal liability for article 312 and 349 offences; and adequately criminalize terrorist financing as a money laundering predicate offense.

Chinese authorities are in the process of addressing several of these deficiencies. China has interpreted its Penal Code to extend the all-crimes offence set out in article 312 to the sole and knowing acquisition and use of proceeds—a judicial interpretations which is poised to become law after undergoing a third reading by the Legal Affairs Committee of the National People's Congress (LAC/NPC). Chinese authorities are amending the Penal Code to provide for corporate criminal liability. A draft Penal Code amendment (Amendment 7) extending corporate criminal liability to article 312 (the all-crimes money laundering offence) passed its first reading at the end of August 2008 but must still undergo second and third readings.

A new anti-money laundering (AML) law, which covers AML/CTF preventative measures for the entire financial system, took effect January 1, 2007. The law extends AML/CTF obligations to the securities and insurance sectors, requires financial institutions to maintain thorough account and transaction records and reports of large and suspicious transactions, and explicitly prohibits financial institutions from opening or maintaining anonymous accounts or accounts in fictitious names. The PBOC remains the primary regulator for AML/CTF purposes for all financial institutions, including insurance and securities, although other regulators (CBRC, CSRC and CIRC) have a role in formulating the requirements, primarily in relation to systems and controls. To implement the new AML Law, PBOC issued "Rules for Anti-Money Laundering by Financial Institutions" (AML Rules) (effective January 1, 2007); "Administrative Rules for Reporting of Large-Value and Suspicious Transactions by Financial Institutions" (LVT/STR Rules) (effective March 1, 2007); and "Administrative Rules for Financial Institutions on Customer Identification and Record Keeping of Customer Identity and Transaction Information (CDD Rules) (effective August 1, 2007). The AML Rules obligate financial institutions to perform customer due diligence, regardless of the type of customer (business or individual), type of transaction, or level of risk. . Under the new regulatory framework, all financial institutions—securities, insurance, trust companies and futures dealers—must manage their own AML mechanisms and report large and suspicious transactions. The LVT/STR Rules were amended on June 21, 2007, to require financial institutions to report suspicious transactions related to terrorist financing.

Under the AML and LVT/STR Rules, banks must report any cash deposit or withdrawal of over renminbi RMB 200,000 (approximately $27,000) or foreign-currency withdrawal of over $10,000 in one business day to the PBOC's financial intelligence unit (FIU). Banks must report either electronically within five days or in writing within 10 days. They must also report money transfers exceeding RMB 2 million (approximately $274,000) between companies in one day or between an individual and a company greater than RMB 500,000 (approximately $68,500). All financial institutions must submit monthly reports describing suspicious activities and retain transaction records for five years. Financial institutions that fail to meet reporting requirements in a timely manner are subject to a range of administrative penalties and sanctions including revocation of their licenses or forced suspension of business operations.

The new CDD Rules require all financial institutions to identify and verify their customers, including the beneficial owner, (although this requirement may be limited to the natural person who ultimately controls—as opposed to owns—a customer), and extend requirements relating to the identification of legal persons to all financial institutions. Banks must identify and verify customers when carrying out occasional transactions over 10,000 RMB or 1,000 U.S. $ equivalent, or when providing cash deposit

or case withdrawal services over 50,000 RMB or 10,000 U.S. $ equivalent. Similar provisions cover a range of cash and other transactions for the insurance sector. All securities transactions must be funded through a custodian bank account subject to CDD. The CDD Rules call for risk-based CDD and monitoring, and introduce specific requirements for financial institutions in relation to foreign Politically Exposed Persons (PEPs), including the requirement to obtain approval from senior management before opening an account and determine the source of funds.

According to Article 16 of China's AML Law, when establishing business relationships, financial institutions must require prospective customers to show a valid identification card or other identification document issued by a reliable independent source. For example, when opening an account, customers who are residents of China must produce an official or temporary identification card, or in the case of military unit servicemen or armed police, an army or police identification card. The financial institution must verify the customer's identity documents by examining their authenticity and keep records of the information contained therein. Financial institutions may also verify the customer's identity through the State Administration of Industry and Commerce (SAIC) or through public security departments. To remedy deficiencies in regulators' ability to obtain information, the PBOC launched a national credit-information system in January 2006. Although still very limited, this system allows banks to have access to information on individuals as well as on corporate entities.

Because of the country's size, the Chinese authorities have evolved a decentralized system of AML/CTF supervision, with general oversight being exercised from PBOC head office in Beijing. The supervisory program includes both onsite and offsite monitoring (based on submission by financial institutions of periodic reports). The frequency of onsite inspections for particular institutions is risk-based. The overall adequacy and effectiveness of China's AML supervisory system is improving, but problems remain, particularly with respect to the usefulness of the offsite process. According to the PBOC 2007 China Anti-Money Laundering Report, examiners executed on-site inspections of 4,533 financial institutions to determine compliance with the AML rules. Of the inspected institutions, 350 received financial sanctions for violating the regulations. The fines totaled RMB 26.52 million (approximately $3.9 million). Of the 350 institutions incurring penalties, 341 were banking financial institutions, 4 were in the securities and futures sector, and the other 5 were in the insurance sector. Of the 350, 347 institutions failed to verify customer identification or report large-value or suspicious transactions, and 3 failed to set up an AML internal control system. Fifty-five percent of the sanctioned institutions were State-owned and joint-stock commercial banks, and 98 percent were Chinese-funded. More recent data is not available.

The AML Law provides for the PBOC's AML authorities, roles and functions, including its FIU. China's FIU is divided into two units within the single overarching authority of the PBOC: China Anti-money Laundering Monitoring & Analysis Center (CAMLMAC) and the Anti-Money Laundering Bureau (AMLB). The heads of CAMLMAC and the AMLB both report to a single deputy governor.

CAMLMAC, established in April 2004, specializes in data collection, processing and analysis, as well as international cooperation. It receives and analyzes STRs and LVTs, and is the central point of contact for foreign FIUs. Established in October 2003, the AMLB organizes and coordinates China's anti-money laundering affairs, and executes administrative investigation, dissemination and policy oversight. Although CAMLMAC and the AMLB work together to conduct follow-up analysis on LVTs and STRs, the AMLB conducts the majority of the additional analysis and dissemination functions.

According to the PBOC, authorities in 2007 discovered 89 cases of money laundering involving RMB 28.8 billion (approximately $4.17 billion). In the first half of 2008, the PBOC sanctioned 12 financial institutions involved in money laundering, with fines totaling RMB 2.25 million (approximately

$329,000), The PBOC has also helped police solve 42 money laundering cases involving about RMB 84.4 billion (approximately $12.4 billion).

The Ministry of Public Security (MPS), China's main law enforcement body, follows up on STRs and guides and coordinates public security authorities across China in money laundering investigations. The AML Division of the MPS Economic Crime Investigation Department (ECID) handles the majority of responsibilities related to the seizing, freezing and confiscation of criminal proceeds. The Anti-Terrorism Bureau of the MPS investigates general crimes relating to terrorist financing. Crimes against state security (including terrorism and related crimes) are the responsibility of the Ministry of State Security (MSS). The Supreme People's Procurator (SPP) supervises and directs the approval of arrests, prosecution, and supervision of cases involving money laundering crimes. The Supreme People's Court (SPC) supervises and directs the trial of money laundering crimes. Both the SPP and the SPC can issue judicial interpretations. Law enforcement agencies have authority to use a wide range of powers, including special investigative techniques, when conducting investigations of money laundering, terrorist financing and predicate offences. These powers include seizing articles relevant to the crime, including all records held by financial institutions. Reportedly, however, law enforcement and prosecutorial authorities focus on pursuing predicate offences, to the exclusion of AML/CTF.

China has implemented a cross-border currency disclosure system using risk-based targeting operated by the General Customs Administration (GCA). All travelers must declare cross-border transportation of cash exceeding RMB 20,000 for local currency (approximately $2,930) or of foreign currency. There is no requirement for bearer negotiable instruments. However, a FATF follow up report states: " China has finished drafting new Administrative Rules on Management of AML Information of Cross-Border Transportation of Cash and Bearer Negotiable Instruments (informal name). The draft is now being circulated among relevant competent authorities for comment. The main issues that are still being debated relate to: (1) reconciling the FATF definition of bearer negotiable instruments with related definitions in existing Chinese legislation; (2) ensuring that the new Rules do not conflict with existing currency-control legislation; and (3) setting the declaration threshold." China prohibits cross-border transportation of RMB through the mail system. The GCA is authorized to conduct checks of persons entering or leaving the country, seize undeclared cash, and question, detain and sanction anyone who violates any requirement. Those who carry out physical cross border transportation related to money laundering or terrorist financing are also subject to criminal sentences. New provisions allowing the use of RMB in Hong Kong have created loopholes for money laundering activity. Authorities do not appear to effectively use captured data for money laundering or terrorist financing investigations.

Only banks have the authority to provide money or value transfer services in China, and may not have agents that offer such services. Article 174 of the Penal Code states that it is a criminal offense to operate an illegal financial institution or provide financial services illegally in China. Although China has had some success at combating illegal underground banking, the country's cash-based economy, combined with robust cross-border trade, contributes to a high volume of difficult-to-track large cash transactions. While China is adept at tracing formal financial transactions, the large size of the informal economy—estimated by the Chinese Government at approximately ten percent of the formal economy, but quite possibly much larger—means that tracing informal financial transactions presents a major obstacle to law enforcement. The prevalence of counterfeit identity documents and underground banks, which in some regions reportedly account for over one-third of lending activities, further hamper AML efforts. Authorities have expressed concern that criminal or terrorist groups could exploit underground banking mechanisms to bypass law enforcement.

The extent of the linkages between underground banking and the large expatriate Chinese community remains unknown. Traditionally, money changers, gold shops, and trading companies operate "flying money" or fei-chien networks. The international Chinese underground banking system depends on close associations and family ties resistant to most law enforcement countermeasures. Value transfer

via trade goods, including barter exchange, is a common component in Chinese underground finance. Many Chinese underground trading networks in Africa, Asia, the Middle East, and the Americas participate in the trade of Chinese-manufactured counterfeit goods, in violation of intellectual property rights. Reportedly, the proceeds of narcotics produced in Latin America are laundered via trade by purchasing Chinese manufactured goods (both licit and counterfeit) in an Asian version of the Black Market Peso Exchange.

To address online fraud, the PBOC has tightened regulations governing electronic payments. PBOC rules prohibit consumers from making online purchases of more than RMB 1,000 (approximately $137) in any single transaction or more than RMB 5,000 (approximately $688) in a single day. Enterprises are limited to electronic payments of no more than RMB 50,000 (approximately $6,900) in a single day. In March 2007, Chinese regulators announced additional online restrictions regarding the use of "virtual money" (online credits sold by websites to customers to pay for games and other web-based services) amidst rumors that criminals were using the credits to launder money.

Terrorist financing is criminalized in Article 120bis of the Penal Code. The MER found that China did not adequately criminalize the sole collection of funds in a terrorist financing context. Through a judicial interpretation of the Penal Code, China has clarified that the terrorist financing offence covers the sole and knowing collection of terrorist funds and has defined "funds" to conform to the definition set forth in the Vienna Convention. These judicial interpretations will likely become law after undergoing a third reading by the Legal Affairs Committee of the National People's Congress (LAC/NPC).

China's primary domestic concerns with terrorist financing focus on the western Xinjiang Uighur Autonomous Region. Subsequent to the September 11, 2001, terrorist attacks in the United States, Chinese authorities began to actively participate in U.S. and international efforts to identify, track, and intercept terrorist finances. However, according to the MER, China has not implemented UNSCR 1267 and UNSCR 1373 in a manner that meets the specific requirements of FATF Special Recommendation III.

China is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. China has signed mutual legal assistance treaties with over 24 countries and has entered into some 70 MOUs and cooperation agreements with over 40 countries. The United States and China signed a mutual legal assistance agreement (MLAA) in June 2000, the first major bilateral law enforcement agreement between the countries. The MLAA entered into force in March 2001 and provides a basis for exchanging records in connection with narcotics and other criminal investigations and proceedings. The United States and China cooperate and discuss money laundering and enforcement issues under the auspices of the U.S./China Joint Liaison Group's (JLG) subgroup on law enforcement cooperation. In addition, the United States and China have established a Working Group on Counterterrorism that meets on a regular basis. China has established similar working groups with other countries as well. China has signed extradition agreements with 30 countries to make it more difficult for economic criminals to seek shelter abroad. According to China's Ministry of Public Security, approximately 800 Chinese economic crime suspects have reportedly fled abroad with more than 70 billion RMB (approximately $9.1 billion) involved. In late 2004, China joined the Eurasian Group on combating money laundering and financing of terrorism (EAG)—a FATF-style regional body. China became a member of the FATF in June 2007.

The Government of China has significantly strengthened its anti-money laundering regime through legislative and regulatory reforms, law enforcement mechanisms, and membership in international organizations, in particular the FATF. The Chinese Government should continue to take steps to develop a viable AML/CTF regime consistent with international standards. China should continue to develop a regulatory and law enforcement environment designed to prevent and deter money

laundering, and it should raise awareness within the judiciary of money laundering as a criminal offense. China should ensure that law enforcement and prosecutorial authorities specifically pursue money laundering and terrorist financing offenses, and not simply treat them as a subsequent byproduct of investigations into predicate offenses. China's Anti-Money Laundering Law and related regulations should also apply to a broader range of nonfinancial businesses and professions. Authorities should assess the application of sanctions for noncompliance with identification, due diligence and record-keeping requirements to ensure that they have a genuinely dissuasive effect. China should ensure that its judicial interpretations that clarify and strengthen its AML/CTF regime become codified in law. In addition to strengthening its counterterrorism finance regime, Chinese law should ensure that it defines the term "terrorist activities" consistently with international standards. The Penal Code should also specify the definition of "funds" and criminalize the act of collecting funds for terrorist purposes. In addition, China should take steps to effectively implement the UNSCRs and strengthen its mechanisms for freezing terrorist assets. Chinese law enforcement authorities should examine domestic and home-grown ties to the international network of Chinese expatriate brokers and traders that often link to underground finance, trade fraud, and trade-based money laundering activities.

Colombia

The Government of Colombia (GOC) is a regional leader in the fight against money laundering. Nevertheless, the laundering of money from Colombia's illicit cocaine and heroin trade continues to penetrate its economy and affect its financial institutions. In addition to drug-related money laundering, laundered funds are also derived from commercial smuggling for tax and import duty evasion, kidnapping for profit, arms trafficking, and terrorism connected to violent paramilitary groups and guerrilla organizations. Further, money laundering is carried out to a large extent by U.S. Government-designated terrorist organizations. An increase in financial crimes not related to money laundering or terrorist financing, such as bank fraud, has not been widely seen in Colombia. However, criminal elements have used the banking sector, including exchange houses, to launder money, under the guise of licit transactions. Money laundering has occurred via trade and the nonbank financial system, especially related to transactions that support the informal or underground economy; the trade of counterfeit items in violation of intellectual property rights is an ever increasing method to launder illicit proceeds. Colombian money is also laundered through offshore centers, generally relating to transactions involving drug-related proceeds. Casinos and free trade zones in Colombia present opportunities for criminals to take advantage of inadequate regulation and transparency. Although corruption of government officials remains a problem, its scope has decreased significantly in recent years.

Colombia's economy is robust and diverse. It is fueled by significant export sectors that ship goods such as coal, petroleum products, textiles and apparel, flowers, and coffee to the United States and beyond. While Colombia is not a regional financial center, the banking sector is mature and well regulated. Comprehensive anti-money laundering regulations, as well as international cooperation on anti-money laundering, have allowed the government to refine and improve its ability to combat financial crimes and money laundering. The GOC and U.S. law enforcement agencies closely monitor transactions that could disguise terrorist finance activities. The United States and Colombia exchange information and cooperation based on Colombia's 1994 ratification of the United Nations Convention against Illicit Trafficking in Narcotics and Psychotropic Substances. This convention applies to most money laundering activities resulting from Colombia's drug trade.

Money launderers in Colombia employ a wide variety of techniques, and frequently use such methods as the Black Market Peso Exchange and contraband trade to launder the proceeds of illicit activities. Colombia's financial intelligence unit (FIU), the Financial Information and Analysis Unit (Unidad de Información y Análisis Financiero or UIAF) has identified more than 44 techniques for laundering

money. Colombia also appears to be a significant destination and transit location for bulk shipment of narcotics-related U.S. currency and European Union euros. Local currency exchangers registered to conduct exchange house transactions, convert narcotics currency to Colombian pesos and then ship U.S. dollars and euros to Europe, Central America and elsewhere for deposit as legitimate exchange house funds that are then reconverted to pesos and repatriated by wire to Colombia. Other methods include the use of debit and stored value cards to draw on financial institutions outside of Colombia and the transfer of funds out of and then back into Colombia by wire through different exchange houses to create the appearance of a legal business or personal transaction. Colombian narcotics traffickers have also been known to coerce local businessmen into purchasing properties, including real property, in "straw" (or nominee) names, which are then leased to unsuspecting tenants. Colombian authorities have had difficulty in prosecuting such schemes for money laundering, and in confiscating such properties under Colombia's extincion de dominio nonconviction based forfeiture law regime. Colombian authorities have also noted increased body smuggling (carrying currency on a person) of U.S. and other foreign currencies, an increase in the number of shell companies operating in Colombia, and rising laundering threats in the real estate and cargo transport sectors. Pre-paid debit and stored value cards, Internet banking, and the dollarization of the economy of neighboring Ecuador represent some of the growing challenges to money laundering enforcement in Colombia. In November 2008, several pyramid schemes collapsed, and the largest alleged scheme was shut down by the Colombian government, under charges of illegal enrichment and suspected money laundering.

Colombia has broadly criminalized money laundering. Under legislation passed in 1995, 1997, and 2001, the GOC has established the "legalization and concealment" of criminal assets as a separate criminal offense, and criminalized the laundering of the proceeds of extortion, illicit enrichment, rebellion, narcotics trafficking, arms trafficking, crimes against the financial system or public administration, and criminal conspiracy. Under a law enacted in 2006, penalties under the criminal code for money laundering and terrorist financing range from eight to 22 years with fines from 650 to 50,000 times the current legal minimum salary. Persons who acquire proceeds from drug trafficking are subject to a potential sentence of six to 15 years, while illicit enrichment convictions carry a sentence of six to ten years. Failure to report money laundering offenses to authorities is itself an offense punishable under the criminal code, with penalties increased in 2002 to imprisonment of two to five years.

Terrorist financing is an autonomous crime in Colombia. Law 1121 of 2006 entered into effect in 2007 which amended the penal code to define and criminalize direct and indirect financing of terrorism, of both national and international terrorist groups, in accordance with the Financial Action Task Force of South America (GAFISUD) and Egmont Group recommendations. The law allows the UIAF to receive STRs regarding terrorist financing, and freeze terrorists' assets immediately after their designation. In addition, banks are held responsible for their client base and must immediately inform the UIAF of any accounts held by newly designated terrorists. Banks also have to screen new clients against the current list of designated terrorists before the banks are allowed to provide prospective clients with services. To fulfill increased monitoring requirements, the GOC increased the size of UIAF staff in 2007 from 45 to 65 positions and authorized the creation of new subdivisions for Information Management and Legal Affairs.

Financial institutions are required by law to maintain records of account holders and financial transactions for five years. Secrecy laws have not been an impediment to bank cooperation with law enforcement officials, since under Colombian law there is a legal exemption to client confidentiality when a financial institution suspects money laundering activity. Colombia's banks have strict compliance procedures, and work closely with the GOC, other foreign governments and private consultants to ensure system integrity. General negligence laws and criminal fraud provisions ensure the financial sector complies with its responsibilities while protecting consumer rights. Obligated entities are supervised by the Financial Superintendent. In 2007, the Financial Superintendent issued a

circular that requires entities under its authority to implement a new consolidated risk-based monitoring system (called SARLAFT) that includes risk prevention and control measures based on international standards. In June 2008, the Financial Superintendent issued a circular effective October 2008 further tightening financial reporting requirements for the financial, insurance, and securities sectors with strict deadlines for submitting regular transaction reports.

Established in 1999 within the Ministry of Finance and Public Credit, the UIAF is widely viewed as a hemispheric leader in efforts to combat money laundering and supplies considerable expertise in organizational design and operations to other FIUs in Mexico, and Central and South America. The UIAF has broad authority to access and analyze financial information from public and private entities in Colombia. Obligated entities, which include banks, stock exchanges and brokers, mutual funds, investment funds, export and import intermediaries, credit unions, wire remitters, money exchange houses, public agencies, notaries, casinos, lottery operators, car dealers, and foreign currency traders, are required to report suspicious transactions to the UIAF, and are barred from informing their clients of their reports. Most obligated entities are also required to establish "know-your-customer" provisions. With the exception of exchange houses, obligated entities must report to the UIAF cash transactions over $5,000. The UIAF requires exchange houses to provide data on all transactions above $200. Between October 2007 and September 2008, 7,980 suspicious transaction reports (STRs) were filed, with 34 percent of STRs deemed by UIAF to merit further investigation by their analysis unit. The Colombian Fiscalia (National Prosecutor's Office) reported 48 convictions for money laundering in 2008.

In 2006, the UIAF inaugurated a new centralized data network connecting 15 governmental entities as well as the private banking association (Asobancaria). The network allows these entities to exchange information online and share their databases in a secure manner, and facilitates greater cooperation among government agencies in preventing money laundering and other financial crimes. As of October 2008, the UIAF's database contained over 709 million transaction and activity reports. Between October 2007 and September 2008, the UIAF provided authorities with 604 financial intelligence reports pertaining to 6,231 individuals, 842 businesses, and approximately $3 billion in transactions. During the same period, UIAF responded to 3,067 information requests from national authorities and 499 requests from Egmont Group members, reducing its response time from an average of eight to three days. The UIAF has also increased its staff from 45 to 65 members, which allows for more and better analysis of financial information.

Given concerns about bulk cash smuggling, the GOC requires individual cash transactions above $5,000 or combined monthly transactions above $50,000 to be handled through the formal financial system, which is subject to the UIAF reporting requirements. It is illegal to transport more than the equivalent of $10,000 in cash across Colombian borders, and the GOC has criminalized cross-border cash smuggling and defined it as money laundering. In spite of improvements, customs officials are inadequately equipped to detect cross-border currency smuggling. Workers rotate frequently producing inadequately trained staff. In addition, the individual customs officials are held liable for any inspected article that they damage, causing hesitation in conducting thorough inspections. Reportedly, corruption is also a problem, and customs officials often lack the proper technical equipment necessary to do their job. The GOC has been slow to make needed changes in this area.

Colombian law provides for both conviction-based and nonconviction based in rem forfeiture, giving it some of the most expansive forfeiture legislation in Latin America. Law 793 of 2002 eliminates interlocutory appeals that prolonged and impeded forfeiture proceedings in the past, imposes strict time limits on proceedings, places obligations on claimants to demonstrate their legitimate interest in property, requires expedited consideration of forfeiture actions by judicial authorities, and establishes a fund for the administration of seized and forfeited assets. The amount of time for challenges is shorter and the focus is on the seized item (cash, jewelry, boat, etc.), placing more burdens on the accused to prove the item was acquired with legitimately obtained resources. Law 785 of 2002, the

National Drug Directorate (DNE) has the authority to conduct interlocutory sales of seized assets and contract with entities for the management of assets. Law 785 also permits provisional use of seized assets prior to a final forfeiture order, including assets seized prior to the enactment of the law. Provisional use has caused some liability issues in Colombia when properties have to be returned for various reasons prior to a final forfeiture.

In spite of improvements to the GOC's asset forfeiture capabilities, a number of problems remain. Concerns about personal liability have discouraged official action in some cases, exceptions in proceedings can still cause cases to drag on for years, and the pace of final decisions remains slow compared to new seizures. Until 2007, prosecutors had limited discretion on asset seizures and had to seize all assets associated with a case, including those of minimal value or those that clearly risk loss under state administration, such as livestock. However, in November 2007, the Attorney General approved pre-seizure guidelines, applicable to forfeitures nationwide, which require an evaluation of an asset's worth prior to seizure, and made other significant changes to the manner in which seizures for forfeiture is conducted. The guidelines were also approved by the DNE Director. With limited resources and only 45 staff dedicated to asset management, the DNE must rely on outside contractors to store or manage assets. The GOC has established priorities for the proceeds of disposed assets; however, DNE's management task will only be reduced when the pace of judicial decisions and disposals exceeds new seizures. The GOC aggressively pursues the seizure of assets obtained by drug traffickers through their illicit activities. In 2008, new regulations were also enacted which permit the DNE to make "interlocutory" sales of assets in some instances, if the values of the properties will deteriorate before final forfeiture can be obtained.

For the last five years, the Sensitive Investigations Unit (SIU) of the Colombian National Police (CNP), in conjunction with U.S. law enforcement and the Colombian Fiscalia have been investigating the Cali and North Valle drug cartels' business empires, including the Rodriguez Orejuela brothers, the Grajales family, and Juan Carlos Ramirez Abadia ("Chupeta"). The Cali and Norte Valle drug cartels, as well as their leaders and associated front persons and businesses, have been named by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) as Specially Designated Narcotics Traffickers (SDNTs), pursuant to Executive Order 12978. The Executive Order imposes financial sanctions against designated targets in order to attack the financial empires built by significant Colombian narcotics traffickers.

Colombian and U.S. law enforcement agencies have cooperated in a series of investigations designed to identify and seize assets either purchased by money gained through illegal drug activity or assets used to launder drug proceeds. In 2008, the Colombian National Police and Colombian Prosecutor's Office seized over 400 assets, including businesses and properties, tied to major Colombian drug trafficker Juan Carlos Ramirez Abadia, bringing the total value of seized cash and assets to nearly $1 billion. These assets included office buildings, a resort hotel, night clubs, and an amusement park. OFAC added additional businesses and front men tied to Chupeta's financial empire to its SDNT list, including a regulated Colombian money exchange business, CAMBIOS Y CAPITALES S.A. These joint actions to seize assets and apply financial sanctions have affected the Colombian drug cartels' abilities to use many of their assets derived from their narcotics trafficking activities and have assisted the Colombian government to pursue major cases to seize narcotics-related assets.

In 2008, several major investigations by DEA and the SIU of the Department of Administrative Security (DAS) resulted in arrests and seizures of major money laundering organizations operating between the countries. These included Operation Titan, which resulted in 113 arrests for money laundering and drug trafficking world wide. Extradition requests to the United States are pending in many of the arrests for Operation Titan and Agents were able to make a direct connection between a traditional Colombian Drug Trafficking and Money Laundering Organization and Middle Eastern money launderers tied to Hezbollah.

The U.S. Department of Homeland Security's Immigration and Customs Enforcement (ICE) has also worked closely with Colombian authorities. In 2002, ICE supported the CNP establishment of a financial investigative unit within the organization's intelligence and investigations unit (DIJIN). The DIJIN has successfully initiated investigations against money laundering organizations in Colombia as well as pursued leads received from on-going U.S. investigations which have resulted in significant arrests and seizures. These include Operation Goldmine, which targeted an organization utilizing textiles as a means to launder narcotics proceeds between the U.S. and Colombia. This investigation led to 32 indictments in the U.S. and the seizure of over $9 million. The DIJIN also successfully targeted the money-laundering infrastructure of Norte Valle Cartel leader Luis Hernando Gomez Bustamante. Coordinating actions with ICE domestic and foreign offices lead to the arrest of high-level members of this organization, which have been extradited to the U.S. from Colombia and other countries, to include its leader. ICE has also helped Colombia establish a Trade Transparency Unit (TTU) with the GOC to aggressively target trade-based money laundering organizations that facilitate the movement of criminal proceeds across borders. TTUs provide a mechanism for the GOC and the USG to identify existing vulnerabilities in both U.S. and foreign financial and trade systems, and to jointly work associated criminal investigations. Colombia's TTU is one of four established foreign TTUs, and includes members from the Directorate of Customs and Revenue (DIAN), UIAF, and DIJIN.

Colombian law is unclear on the government's authority to block assets of individuals and entities on the UN 1267 Sanctions Committee consolidated list. The government circulates the list widely among financial sector participants, and banks are able to close accounts but not seize assets. Banks also monitor other lists, such as OFAC's publication of Specially Designated Terrorists. Charities and nongovernmental organizations (NGOs) are regulated to ensure compliance with Colombian law and to guard against their involvement in terrorist activity. This regulation consists of several layers of scrutiny, including the regulation of incorporation and the tracing of suspicious financial flows through the collection of intelligence or STRs.

The GOC is a member of GAFISUD. However, as a result of the GOC's failure to pay its membership dues dating back to 2004 (totaling approximately $87,000), the GOC's participation in GAFISUD-sponsored events is limited, and the GOC does not have a voice at GAFISUD plenary meetings. According to GOC officials, new legislation is required to authorize the GOC to pay its membership dues; past dues had been paid without legal authorization. In April 2008 the Colombian Congress passed Law 1186 to authorize future payments to GAFISUD. However, at the time of this report, the Constitutional Court had referred the legislation back to the Congress for republication before final constitutional approval—a process expected to take several months. A Mutual Evaluation (ME) by GAFISUD of Colombia was conducted during June 30 to July 9, 2008. Overall, Colombia's AML/CTF regime complies with the FATF 40 Recommendations and the Nine Special Recommendations.

Colombia is a member the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Money Laundering Experts Working Group. The UIAF is a member of the Egmont Group, and has signed memoranda of understanding with 27 FIUs, and in August 2008, proposed concluding a regional memorandum of understanding with 11 Caribbean Basin countries as well as promoted the incorporation of money laundering and terrorism financing provisions into the Cartagena Declaration of the Regional Counternarcotics, Security and Cooperation Summit. The GOC also issued presidential joint statements with Paraguay and Honduras in 2008 to strengthen cooperation between respective FIUs. In 2008, UIAF organized nine international workshops, which trained more than 220 officials from Ecuador, Peru, Bolivia, and Paraguay. The GOC is a party to the1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Corruption, and the UN Convention against Transnational Organized Crime. The GOC has signed, but not yet ratified, the Inter-American Convention against Terrorism.

In 2008, the Government of Colombia made additional progress in the development of its financial intelligence unit, regulatory framework and interagency cooperation within the government. The further strengthening and broadening of financial reporting requirements reinforce efforts to fight terrorism and financial crime. International cooperation with the U.S. and other countries has led to several high-profile seizures and prosecutions. The transition to a new criminal procedure provides potential for improved use of undercover and other critical investigative techniques, as well as increasing the possibility of plea bargaining and the use of confidential investigations. However, this new system is still being learned. Greater focus and priority toward money laundering investigations, including increased resources, are needed to ensure greater progress. The growth in contraband trade to launder illicit drug proceeds will require even greater interagency cooperation within the GOC, including coordination between the UIAF and DIAN, Colombia's Trade Transparency Unit, and the tax and customs authority. Congestion in the court system, procedural impediments and corruption remain problems. Limited resources for prosecutors, investigators, and the judiciary hamper the ability to close cases and dispose of seized assets. Further, streamlined procedures for the liquidation and sale of seized assets under state management could help provide funds available for Colombia's anti-money laundering and counterterrorist financing regime. The GOC is also strongly encouraged to enact legislation to permit the use of proceeds from confiscated assets to support its law enforcement efforts. In addition, the GOC should ensure that the necessary legislation is passed to allow it to pay its GAFISUD dues and become active in GAFISUD once again.

Comoros

The Union of the Comoros (Comoros) consists of three islands: Grande Comore, Anjouan and Moheli. Although Comoros lacks homegrown narcotics, the islands are used to transit drugs, mainly from Madagascar. The presidency of the Union rotates between the three islands. An ongoing struggle for influence between the Union and the island presidents continued into 2008.

Comoros is not a principal financial center for the region. An anti-money laundering (AML) law addressing many of the primary AML issues of concern was passed by Presidential Decree in 2004. However, the 2004 law does not meet international standards. Also, while legally applicable to all three islands, the AML law was not enforced on Anjouan prior to March 2008. In addition, Comoran authorities lack the capacity to effectively implement and enforce the2004 AML law, as the three islands in the Comoros retain a great deal of autonomy, particularly with respect to their security services, economies, and banking sectors.

In 2007 Comore and Moheli held free elections. However, Colonel Mohamed Bacar refused to hold elections in Anjouan. In June 2007, Anjouan, under the leadership of Colonel Mohamed Bacar, de facto seceded from the Union. Union President Ahmed Abdallah Mohamend Sambi and his cabinet were unable to govern Anjouan. On March 25, 2008, a joint Union of the Comoros and African Union military force removed Colonel Bacar and restored Union legal authority and order.

Both Moheli, pursuant to the International Bank Act of 2001, and Anjouan, pursuant to the Regulation of Banks and Comparable Establishments of 1999, licensed more than 300 offshore banks. Neither island required applicants for banking licenses to appear in person to obtain their licenses. Anjouan required only two documents (a copy of the applicant's passport and a certificate from a local police department certifying the lack of a criminal record) to obtain an offshore license and accepted faxed copies of the required documents. In addition to licensing shell banks, Anjouan sold the right to issue bank licenses. All of the shell banks and other entities were located offshore and had no permanent presence in the Comoros. Neither jurisdiction had the expertise or resources to effectively regulate an offshore banking center. Anjouan delegated most of its authority to operate and regulate the offshore business to private, non-Comoran domiciled parties.

In addition to offshore banks, both Moheli, pursuant to the International Companies Act of 2001, and Anjouan, pursuant to Ordinance Number 1 of 1 March 1999, licensed insurance companies, internet casinos, and international business companies (IBCs). Moheli claims to have licensed over 1200 IBCs. Moheli law permits bearer shares of IBCs. Anjouan also allows trusts, and will register aircraft and ships without requiring an inspection of the aircraft or ship in Anjouan.

The Union Central Bank retains a French financial professional as "Financial Controller," and corresponds with French commercial banking authorities. Central Bank Governor Abdoulbastoi sent the United States a comprehensive report on Union Government policies and actions with regard to Anjouan illicit banking activities. The Union Central Bank published informational circulars intended to warn members of the international financial system against dealings with banks "licensed" by Anjouan. The circulars explained that offshore and onshore financial institutions operating within the jurisdiction of the Union of the Comoros must abide by the provisions of legislation No. 80-7 of May 3, 1980, which requires that a financial institution operating in the Union of the Comoros receive prior authorization from the Union Finance Minister upon recommendation from the Comoros Central Bank. Therefore, offshore banks operating in the autonomous islands of the Union of the Comoros without prior authorization from the Union Finance Minister were operating illegally. Because the involved computer servers and illicit "entities" are located outside the Comoros, the GOC lacks the jurisdiction and capacity to act beyond the announcements and warnings regarding the illegal entities.

Citing the law conferring sole authority for granting banking licenses on the Union Central Bank, the Governor asked financial authorities in France, Belgium, and the United States to prohibit all activities within their jurisdictions by Anjouan-registered entities. Union President Sambi also requested international assistance in closing any shell banks or illicit financial entities that operate within the Comoros without legitimate approval. The Governor repeated an earlier request to U.S. and European authorities for help closing all websites associated with Anjouan. The government also issued numerous public announcements warning the public against Anjouan financial entities. A regularly-updated circular lists the banks properly accredited by the Union Central Bank in the Comoros: Central Bank of Comoros, Commerce and Industry Bank, Comoros Development Bank, National Post Office and Financial Services Company, Meck Union, and Sanduk Union. The Ex-Im Bank, a Tanzanian entity, opened in 2008.

Since Bacar fled to Benin and is no longer in power in Anjouan, Union authorities report that these illicit activities have ceased in Anjouan. During 2008, Comoros closed many of the illegitimate financial institutions, and Moheli and Anjouan no longer issue banking licenses to offshore entities. Current legal licensing authority rests with the Union Finance Minister and Union Central Bank Governor, and the Anjouan and Moheli counterparts are under Union control. However, the already established offshore entities remain outside Union control. The entity to which the Anjouan authorities sold licensing authority may still be issuing licenses in the name of Anjouan. The Comoran government has solicited the law enforcement authorities in the United Kingdom and France to locate and arrest the perpetrators, who were reportedly in Europe.

In early 2007, Union Vice President Idi Nadhoim hosted a World Bank- Bank of France seminar on policies to combat money laundering and terrorist finance. Union Central Bank officials, commercial banks, and operators participated.

As of December 2008, the Union had a draft of a new AML law before the Parliament. Until that law is promulgated, Comoros will use its 2004 federal-level AML law, based on the French model. The 2004 law requires financial and related records to be maintained for five years; permits assets generated or related to money laundering activities to be frozen, seized and forfeited; requires residents to declare all currency or financial instruments upon arrival and departure, and nonresidents to declare all financial instruments upon arrival and all financial instruments above Comoran francs 500,000 (approximately $1,250) on departure; permits provision and receipt of mutual legal assistance

with another jurisdiction where a reciprocity agreement is in existence and confidentiality of financial records is respected; requires nonbank financial institutions to meet the same customer identification standards and reporting requirements as banks; requires banks, casinos and money exchangers to report unusual and suspicious transactions (by amount or origin) to the Central Bank and prohibits cash transactions over Comoran francs 5 million (approximately $12,500); and criminalizes the provision of material support to terrorists and terrorist organizations. In addition, there is a suspicious activity filing requirement in the Union's AML law, and reports go to the Central Bank, as stipulated in the law. Comoros does not have an operational financial intelligence unit (FIU).

Foreign remittances from Comorans living abroad in France, Mayotte (claimed by France) and elsewhere remain the most important influx of funds for most Comorans. A 2008 African Development Bank report estimated total annual remittances at $100 million, with two-thirds arriving via informal means. In 2006, Western Union established a presence in Comoros to capture part of this market, but most Comorans continue to prefer to use informal sectors.

As mentioned above, Union authorities have limited ability to implement AML laws in Anjouan and Moheli due to the islands' degree of autonomy. Similarly, the island governments of Anjouan and Moheli may have limited control over AML matters. Although Moheli has its own AML law in effect (the Anti-Money Laundering Act of 2002), the law itself has serious shortcomings and authorities lack the resources and expertise to enforce its provisions. Comprehensive information on Anjouan's laws and regulations is difficult to obtain, but it appears Anjouan does have an AML law (the Money Laundering Prevention Act, Government Notice 008 of 2005). However, little is known about: (i) the procedures that have been established to review and approve offshore licenses issued before the enactment of the AML law; (ii) the procedures that have been established to review and approve ongoing bank license applications and to supervise and monitor institutions for compliance with Anjouan laws; and (iii) the efforts and resources available to implement these procedures and enforce compliance.

President Sambi has reiterated Union Government support for efforts to bring AML enforcement under Union government jurisdiction. These efforts include the drafting of the new AML legislation currently under consideration by Parliament and the prosecution of corrupt former officials. A grossly inadequate budget, dysfunctional ministries, and a nonfunctioning judiciary limit effectiveness. The lack of capacity severely hinders progress on AML issues, despite apparent high-level political support.

France, the former colonial power, maintains substantial influence and activity in Comoros and, where possible, has bypassed the Union and island governments to prosecute suspected money launderers or shell banks under French law.

Comoros is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism.

Comoros is a member of the free-trade area of the Common Market for Eastern and Southern Africa (COMESA). It has obtained observer status in the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. The Comoros is moving toward full membership in ESAAMLG, which will commit Comoros to adherence to the FATF's international standards. Comoros has agreed to an on-site visit by ESAAMLG, scheduled to take place in early 2009, and a mutual evaluation visit by the IMF, scheduled for May 2009.

The Government of the Union of the Comoros (GOC) should ensure that the draft anti-money laundering legislation meets international standards, and pass the legislation, which will apply to the three islands that comprise the federal entity. Authorities should ensure that their activities relating to the implementation of the law, when promulgated, take place in all three islands. Authorities should

establish an FIU with jurisdiction over the entire country and prohibit bearer shares. Authorities should circulate the list of individuals and entities that are included on the United Nations 1267 Sanctions Committee's consolidated list to Comoran banks. With a total annual operating budget of the Union Finance Ministry less than $100,000, Comoran authorities should ensure that resources target FIU development and regulatory and law enforcement capacity.

Cook Islands

The Cook Islands is a self-governing parliamentary democracy in free association with New Zealand and a member of the British Commonwealth. The Cook Islands' offshore sector makes it vulnerable to money laundering, as the sector offers banking, insurance, and formation of international business companies and trusts. However, due to recent legislative and regulatory changes, the Cook Islands comply with current international standards.

The domestic banking system is comprised of branches of two major Australian banks and the local Bank of the Cook Islands (BCI). Domestic banks are primarily involved in traditional deposit taking and lending. The BCI operates as a stand-alone institution competing against the two Australian banks and is no longer engaged in development lending. Legislation allows for development lending to be undertaken in the future by a separate company not subject to supervision by the Financial Supervisory Commission (FSC). In addition to the three domestic banks, the Cook Islands financial sector also consists of four international banks, six trustee companies, and three offshore and three domestic insurance companies. The domestic insurance companies are not regulated by the FSC, but legislation has been enacted to allow regulation to take place from1 January 2009.

The Cook Islands has an offshore financial sector that licenses international banks and offshore insurance companies and registers international business companies (IBCs). The offshore sector also consists of company services and trusts, including asset protection trusts (APTs). APTs protect the assets of individuals from civil judgments in their home countries and are able to contain a "flee clause." It is possible, that under a "flee clause," if a foreign law enforcement agency makes an inquiry regarding the trust, the trust will be transferred automatically to another offshore center. According to officials of the Government of the Cook Islands (GOCI), the "flee clause" exists to transfer APTs in times of emergency, such as a natural disaster, but they may also incorporate clauses designed to avoid the courts of the jurisdiction they are in or investigations by regulatory authorities. In practice they are rarely used, as they are difficult to implement without the trustee finding itself in breach of Cook Islands law.

The Cook Islands was placed on the Financial Action Task Force (FATF) list of Non-Cooperative Countries and Territories (NCCT) in 2000. After the GOCI addressed deficiencies in its anti-money laundering regime by enacting legislative reforms, the FATF removed the Cook Islands from its NCCT list in February 2005. The FATF conducted a year-long monitoring program, which concluded in June 2006, to closely monitor the islands.

The Banking Act 2003 and the Financial Supervisory Commission Act (FSCA) 2003 established a new framework for licensing and prudential supervision of domestic and offshore financial institutions in the Cook Islands. The legislation requires international offshore banks to have a physical presence in the Cook Islands, transparent financial statements, and adequate records prepared in accordance with consistent accounting systems. The physical presence requirement is intended to prohibit shell banks. All banks are subject to a vigorous and comprehensive regulatory process, including on-site examinations and supervision of activities.

The FSCA established the Financial Supervisory Commission as the licensed financial sector's sole regulator. The FSC is empowered to license, regulate, and supervise the business of banking. It serves as the administrator of the legislation that regulates the offshore financial sector. The FSC can license

international banks and offshore insurance companies and register international companies and limited liability companies. It also supervises trust and company service providers. Its policy is to respond to requests from overseas counterparts to the utmost extent possible. The FSC has taken a broad interpretation of the concept of "counterpart" and does not need to establish general equivalence of function before being able to cooperate.

Licensing requirements, as set out in the legislation, are comprehensive. The Banking Act 2003 and a Prudential Statement on Licensing issued in February 2004 contain detailed licensing criteria for both locally incorporated and foreign banks, including "fit and proper" criteria for shareholders and officers, satisfactory risk management, accounting and management control systems, and minimum capital requirements. The Banking Act 2003 defines banking business, prohibits the unauthorized use of the word "bank" in a company name, and requires prior approval for changes in significant shareholding.

By enacting the Financial Transactions Reporting Act (FTRA) 2004, which replaced a similar Act passed a year earlier, the Cook Islands authorities strengthened its anti-money laundering and counterterrorist financing (AML/CTF) legal and institutional framework. The threshold approach of serious offenses is 12 months imprisonment or $5,000 fine. The Financial Supervisory Commission (FSC) supervises and examines financial institutions for compliance with anti-money laundering laws jointly with the Financial Intelligence Unit (FIU). Reviews are underway to consider how the AML/CTF legislation affects other domestic laws. The legislation regulates the small domestic insurance sector and update supervision of the offshore insurance sector. Insurance intermediaries will also be regulated under the proposed legislation.

The FTRA imposes certain reporting obligations on 26 different types of institutions, including banks, offshore banking businesses, offshore insurance businesses, casinos, gambling services, insurers, financial advisors, solicitors/attorneys, accountants, financial regulators, lotteries, money remitters, motor vehicle dealers, dealers in precious metals and stones, and friendly societies. The Minister of Finance can extend the reporting obligation to other businesses when required. Reporting institutions are required to retain all records related to the opening of accounts and financial transactions for a minimum of six years. The records must include sufficient documentary evidence to verify the customer's identity. In addition, reporting institutions are required to develop and apply internal policies, procedures, and controls to combat money laundering and to develop audit functions to evaluate such policies, procedures, and controls. Reporting institutions must comply with any guidelines and training requirements issued under the FTRA, as amended, and must provide internal training on all anti-money laundering matters. The FTRA provides for administrative and financial sanctions on institutions for noncompliance.

The FTRA requires the FSC to assess the compliance by licensed financial institutions with customer due diligence and record keeping requirements. Resulting reports and documentation from annual inspections are provided to the Cook Islands Financial Intelligence Unit (CIFIU) and the FIU decides if any matters are to be referred for prosecution. The CIFIU is also responsible for assessing compliance by nonlicensed institutions.

The CIFIU is an independent ministry of the Cook Islands Government and is the central unit responsible for the collection, analysis and dissemination of financial information and intelligence on suspected money laundering, terrorist financing and other serious offences to the appropriate authorities in the Cook Islands. The Cook Islands Police are responsible for investigating financial crimes, including money laundering and terrorist financing. The CIFIU is responsible for the supervision of all registered Reporting Institutions in the Cook Islands, as required by the Financial Transactions Reporting Act 2004. For financial institutions this responsibility is shared with the FSC, but is the sole responsibility of the FIU for DNFBPs. In 2008, the CIFIU received 30 STRs; 3,130 CTRs; 2 Border Currency Reports and 6,384 Electronic Funds Transfer Reports, which resulted in a

total of 2 intelligence reports. There have been no seizures and/or confiscations related to money laundering or terrorist financing to date.

The FTRA 2004 grants supervisory authority to the CIFIU, allowing it to cooperate with other regulators and supervisors, require reporting institutions to supplement reports, and obtain information from any law enforcement agency and supervisory body. To facilitate information exchange within Cook Islands' borders, the FIU has signed domestic MOUs with the FSC, Cook Islands Police, as well as Customs and Immigration.

Obligated institutions are required to report any attempted or completed large currency transactions and suspicious transactions to the CIFIU. The currency reporting requirements apply to all currency transactions of NZ$10,000 (approximately $6870) and above, electronic funds transfers of NZ$10,000 and above, and transfers of currency in excess of NZ$10,000 into and out of the Cook Islands. Failure to declare such transactions could incur penalties. The CIFIU is required to destroy a suspicious transaction report if there has been no activity or information related to the report or to a person named in the report for six years. The CIFIU does not have an investigative mandate. If it determines that a money laundering offense, serious offense or terrorist financing offense has been or is being committed; it must refer the matter to law enforcement for investigation. The Attorney General, who is responsible for administrative oversight, appoints the head of the CIFIU.

Cross border movement of cash in and out of the Cook Islands is criminalized under the Proceeds of Crime Act for cash and negotiable bearer instruments over $10,000. Border Cash reports are submitted to the FIU and if the information requires further dissemination, it would be disseminated to the appropriate agency for analysis. However, to date, there has not been any necessity for dissemination of information.

Since June 2004 the Cook Islands had made further progress in implementing its AML/CTF regime. The head of the CIFIU chairs the Coordinating Committee of Agencies and Ministries, which promotes, formalizes and maintains coordination among relevant government agencies; assists the GOCI in the formulation of policies related to AML/CTF issues; and enables government agencies to share information and training resources gathered from their regional and international networks. The AML/CTF consultative group of stakeholders facilitates consultation between government and the private sector, and ensures all financial sector players are involved in the decision making and problem solving process regarding AML/CTF regulations and reporting. The CIFIU is also a member of the Anti-Corruption Committee, along with the Office of the Prime Minister, Police, Crown Law, Audit Office, and the Financial Secretary.

The Terrorism Suppression Act 2004, based on the model law drafted by an expert group established under the auspices of the Pacific Islands Forum Secretariat, criminalizes the commission and financing of terrorism. The United Nations (Security Council Resolutions) Act 2003 allows the Cook Islands, by way of regulations, to give effect to the Security Council resolutions concerning international peace and security.

The Cook Islands is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention for the Suppression of the Financing of Terrorism. The Cook Islands is not a party to the UN Convention Against Corruption.

The Cook Islands is an active member of the Asia/Pacific Group on Money Laundering (APG) and the CFIU is a member of the Egmont Group. The CFIU has bilateral agreements allowing the exchange of financial intelligence with Australia, New Zealand, Philippines, Chinese Taipei, Vietnam and the Philippines. The Cook Islands is still negotiating a memorandum of understanding (MOU) with Thailand and is in the process of signing Mutual Legal Assistance Agreement with Poland. The Cook Islands plans to become a member of the Offshore Group of Banking Supervisors (OGBS), once it has qualified by undergoing further evaluation. The GOCI is an active member of the Association of

Financial Supervisors of Pacific Countries and draws on the resources of this association and Pacific Financial Technical Assistance Centre for capacity building for FSC staff. The Cook Islands has no free trade zones; and participates in the Pacific Island Countries Trade Agreement (PICTA).

The Cook Islands has received nine requests for mutual legal assistance since the Mutual Assistance in Criminal Matters Act came into force in 2003. Six have been answered, and three are pending. The Cook Islands has not received any extradition requests from foreign countries, but successfully extradited one person from New Zealand.

The Cook Islands cooperates with the international community on all money laundering, financial crimes, and terrorist related financing issues. The UN 1267 sanction committee's consolidated list of individuals and entities has been circulated to financial institutions. No accounts with names or entities listed on the UN list are being maintained with any financial institutions in the Cook Islands.

The Government of the Cook Islands should maintain vigilant regulation of its offshore financial sector, including its asset protection trusts, to ensure that its offshore sector continues to comport with international standards. The GOCI should enact and implement Border Currency Reporting legislation, Civil Forfeiture legislation, and a Risk Based Money Laundering and Terrorist Finance regulation, together with amendments to the Financial Transactions Reporting Act and the Terrorism Suppression Act. The Government should continue to monitor alternative money service businesses, and enact legislation governing such businesses in the event that transaction volumes in alternative money services increase. Doing so would further ensure that the GOCI's status as a low risk AML/CTF jurisdiction that could serve as model for other Pacific Island jurisdictions.

Costa Rica

Costa Rica is not a major regional financial center but does have an offshore financial sector and remains vulnerable to money laundering and other financial crimes Illicit proceeds of narcotics trafficking (mainly cocaine); fraud; trafficking in persons, arms trafficking; corruption; and unregulated Internet gaming companies likely are laundered in Costa Rica. Bank fraud, especially via the Internet, appears to be on the rise, though there has not been a rise in use of counterfeit currency. While local criminals are active, the majority of criminal proceeds laundered derive primarily from foreign criminal activity. In 2002, the Government of Costa Rica (GOCR) enacted Law 8204 that supersedes a prior law that only criminalized narcotics-related money laundering. Law 8204 criminalizes the laundering of proceeds from all serious crimes, which are defined as crimes carrying a sentence of four years or more. While Law 8204, in theory, applies to the movement of all capital, current regulations are narrowly interpreted so that the law applies only to those entities that are involved in the transfer of funds as a primary business purpose, such as banks, exchange houses and stock brokerages. Therefore, the law does not cover such entities as casinos, dealers in jewels and precious metals, insurance companies, intermediaries such as lawyers, accountants or broker/dealers, or Internet gambling operations, as their primary business is not the transfer of funds.

Costa Rican financial institutions are regulated by the Superintendent General of Financial Entities (SUGEF), Superintendent General of Securities (SUGEVAL), and the Superintendent of Pensiones (SUPEN). All three entities fall under the National Council of Supervision of the Financial System (CONASSIF). Law 8204 also established Costa Rica's financial intelligence unit (FIU), the Unidad de Analisis Financiero (UAF). The law obligates financial institutions and other businesses to identify the beneficial owners of all accounts; retain financial records for at least five years; and, to report currency transactions over $10,000 and suspicious transactions, regardless of the amount involved or transaction to the UAF. Law 8204 does not establish any protection for reporting individuals, however failure to file suspicious transaction reports (STRs), can result in monetary sanctions established in Article 81 of the law. The UAF requests, collects and analyzes STRs submitted by obligated entities and cash transaction reports (CTRs) it receives.

The UAF has no regulatory responsibilities. The UAF has access to the records and databases of financial institutions and other government entities, but the Judicial Investigative Organization (OIJ) must obtain a court order if the information collected is to be used as evidence in court. Additionally, there are formal mechanisms in place to share information domestically and with other countries' FIUs. In spite of its broad access to government information and high levels of cooperation with the financial sector, the UAF is somewhat ill-equipped and under-funded to provide information needed by investigators. In 2009, the UAF plans to hire four additional forensic auditors, and one investigator to bring total staffing to 27. In 2008, the UAF continued to increase the quality of its analysis and forwarded more thoroughly analyzed cases to prosecutors. In 2008, the UAF received 500 STRS and forwarded 36 to the Unidad de Investigacion Financiero (UIF) of the Money Laundering, Financial, and Economic Crimes Unit, the OIJ, under the Public Ministry (Prosecutor's Office); the entity responsible for investigating financial crimes. The OIJ is assisted by the UAF and has adequately trained staff. In 2008, there were two prosecutions for financial crime.

The UAF does not directly receive CTRs. Each superintendence that receives CTRs holds the CTRs until it determines that further analysis is required or until the UAF requests the CTRs. After analysis, if the UAF thinks that a CTR warrants further investigation, the CTRs would be forwarded to the UIF for investigation.

The GOCR reports that Costa Rica is primarily used as a bridge to send funds to and from other jurisdictions using, in many cases, companies or established banks in offshore financial centers. All persons carrying, entering or exiting Costa Rica are required to declare any amount over $10,000 to Costa Rican officials at ports of entry. Declaration forms are required. Cash smuggling reports are entered into a database maintained by ICD and is shared with appropriate government agencies, including the UAF. The OIJ reports that currency smuggling has increased at land borders; also, money laundering may be occurring through the use of wire-transfer services. Alternative remittance systems exist in Costa Rica, mainly as a result of Costa Rican migration to the United States, or Nicaraguans to Costa Rica. However, there is no confirmation that these remittance systems are used for money laundering. Remittances as of June 2008 totaled approximately $589 million. According to the GOCR, there is a black market for smuggled goods in Costa Rica, but the size is not known. There is no particular evidence that it is being funded by narcotics or other illicit proceeds.

There are 28 free trade zones (FTZs) within Costa Rica, used by approximately 250 companies. The Promotora del Comercio Exterior de Costa Rica (PROCOMER) manages the FTZ regime and has responsibility for registering all qualifying companies. PROCOMER's qualification process consists of conducting due diligence on a candidate company's finances and assessing the total cost of ownership. PROCOMER annually audits all of the firms within the FTZ regime and touts its system of tight controls aimed primarily at preventing tax evasion. The four major types of firms operating under Costa Rica's FTZ regime are manufacturing, professional services, trading, and administrative organizations. PROCOMER reports that there was no evidence of money laundering activity in the FTZs in 2008.

While the formal banking industry in Costa Rica is tightly regulated, the offshore financial sector, which offers banking, corporate and trusts formation services, remains an area of concern. Foreign-domiciled offshore banks can only conduct transactions under a service contract with a domestic bank, and they do not engage directly in financial operations in Costa Rica. They must also have a license to operate in their country of origin. Furthermore, they must comply with Article 146 of the Costa Rican Central Bank's Organic Law, which requires offshore banks to have assets of at least $3 million dollars, a physical presence in Costa Rica, and be subject to supervision by the banking authorities of their registered country. Shell banks are not allowed in Costa Rica and regulated institutions are forbidden from having any direct or indirect relationships with institutions that may be described as shell banks or fictitious banks. Bearer shares are not permitted in Costa Rica. Currently, six offshore banks maintain correspondent operations in Costa Rica: three from the Bahamas and three from

Panama. There are memoranda of understanding (MOUs) between Costa Rica and Panama and the Bahamas to allow easy information exchanges. The GOCR has supervision agreements with its counterparts in both countries, permitting the review of correspondent banking operations. However, these counterpart regulatory authorities occasionally interpret the agreements in ways that limit review by Costa Rican officials. In 2005, the Attorney General ruled that the SUGEF lacked authority to regulate offshore operations due to an apparent contradiction between the 1995 Organic Law of the Costa Rican Central Bank and Law 8204, the primary anti-laundering legislation criminalizing the laundering of proceeds from all serious crime. Draft legislation to correct the contradiction and reassert the SUGEF's regulatory power was submitted to the national assembly for consideration in 2008. Purportedly, additional but unspecified actions by SUGEF should decrease the number of offshore banks in the next year.

Gambling is legal in Costa Rica, and in April of 2008, five government decrees established new rules to better identify casino ownership and regulate operations. None addressed online casinos and there is no requirement that the currency used in Internet gaming operations be transferred to Costa Rica. There are over 250 Internet sports-book companies registered to operate in Costa Rica. In January 2008, the United States charged 12 individuals with money laundering and gambling offenses related to the operation of a Costa Rican based gambling website and call center that serviced sports books in the U.S.

Articles 33 and 34 of Law 8204 cover asset forfeiture and stipulate that all movable or immovable property used in the commission of crimes covered by this act shall be subject to preventative seizure. When asset seizure or freeze takes place, the property is placed in a legal deposit under the control of ICD. The banking industry closely cooperates with law enforcement efforts to trace funds and seize or freeze bank accounts. During 2008, officials seized over $2 million in narcotics-related assets, much of it in undeclared cash. Seized assets are processed by the ICD and if judicially forfeited, are divided among drug treatment agencies (60 percent), law enforcement agencies (30 percent), and the ICD (10 percent) or as determined by ICD's council. It is unclear whether GOCR will assist other countries in obtaining nonconviction-based forfeiture since its domestic laws only provide for conviction-based forfeiture.

Although Costa Rica is a party to the major United Nations counterterrorism conventions, including the UN Convention for the Suppression of the Financing of Terrorism, terrorist financing is not yet a crime in Costa Rica. In 2002, a government task force drafted a comprehensive counterterrorism law with specific terrorist financing provisions that has not been enacted. However, a draft of Bill 17009, expected to be enacted in February 2009, explicitly criminalizes the financing of terrorism, and will obviate the expulsion of the UAF from the Egmont Group

Costa Rican authorities receive and circulate to all financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to Executive Order (E.O.) 13224. However, these authorities cannot block, seize, or freeze property without prior judicial approval. Costa Rica lacks the ability to expeditiously freeze assets connected to terrorism.

No assets related to designated individuals or entities were identified in Costa Rica in 2008. Yet, according to the Government of Costa Rica (GOCR) there is some evidence of FARC (Revolutionary Armed Forces of Colombia) money laundering operations here. In a high-profile incident in March 2008, a prominent couple from the Costa Rican academic community was found with a safe containing $480,000 in FARC money. The couple was also involved in a real estate transaction on behalf of a prominent FARC leader, which to date has not been investigated.

Costa Rica fully cooperates with appropriate United States government law enforcement agencies and other governments investigating financial crimes related to narcotics and other crimes. Articles 30 and

31 of Law 8204 grant authority to the UAF to cooperate with other countries in investigations, proceedings, and operations concerning financial and other crimes covered under that law.

Costa Rica is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. The GOCR is a member of the Money Laundering Experts Working Group of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD). Costa Rica is a member of the Caribbean Financial Action Task Force (CFATF), a Financial Action Task Force (FATF) style regional body. The CFATF conducted a mutual evaluation of Costa Rica in 2006. During the CFATF Plenary in St. Kitts and Nevis in November 2008, the GOCR reported on actions taken to comply with recommendations made by the team of experts who evaluated the GOCR's anti-money laundering regime in 2006. There were modifications to Bill 17009 and 8204 to clarify the filing of STRs to the UAF, among others. However, the GOCR may still need to amend its laws to provide for a "safe harbor" protection for those who submit suspicious AML/CTF activity reports.

The GOCR should pass legislation that reconciles contradictions regarding the supervision of its offshore banking sector. With the expected passage of the terrorism bill 17009 the loopholes in anti-money laundering legislation, regulations to cover the Internet gaming sector, dealers in jewelry and precious metals, intermediaries such as lawyers, accountants or broker/dealers, casinos, as well as any business activity that might entail the use of cash and other nonbank financial institutions, should be addressed. The GOCR should also consider either adopting civil forfeiture, or, at a minimum, clarify in law or regulation that it can assist other countries with forfeiture when a conviction has been obtained even if the forfeiture is not part of the criminal proceeding. Finally, Costa Rica should ensure that its financial intelligence unit and law enforcement agencies authorities are adequately equipped to combat financial crime.

Côte d'Ivoire

The Republic of Cote d'Ivoire is an important West African regional financial hub. Money laundering in Cote d'Ivoire is not primarily related to narcotics proceeds. Criminal proceeds that are laundered are reportedly derived from regional criminal activity, such as the smuggling of consumer goods and agricultural products. Reportedly, most of the smuggling networks are organized chiefly by nationals from Nigeria and the Democratic Republic of the Congo. Due to the ongoing political and economic turmoil in Cote d'Ivoire, rule of law implementation remains poor. As a result, Ivorian and other West African nationals are becoming increasingly involved in criminal activities and the subsequent laundering of illicit funds. Public corruption, including embezzlement of public funds and the laundering of those funds also pose concerns. The extent to which Ivorian territory is used in the growing use of West Africa as a transshipment point for drugs from South America to Europe is largely unknown but is of concern to law-enforcement officials. Ivorian law enforcement authorities have little control over the northern half of the country. The ongoing de facto division of the country makes it difficult to assess Ivorian involvement in narcotics trafficking, as well as Cote d'Ivoire's possible role as a center for the laundering proceeds from narcotics trafficking.

The outbreak of the rebellion in 2002 increased the amount of smuggling of goods across the northern borders, including cocoa, cashews, timber, textiles, tobacco products, and light motorcycles. Reportedly, there has also been an increase in the processing and smuggling of diamonds from mines located in the north. National authority is slowly redeploying, but the government's control over borders in the formerly rebel-controlled regions of the country remains very weak. The relationship between revenues associated with smuggled goods and narcotics proceeds remains unclear due to the lack of effective border controls in the north. Smuggling of sugar, cotton, cocoa, coffee, cars, and pirated DVDs occurs in the government-controlled south and is motivated by a desire to avoid the payment of taxes (principally value-added taxes). According to the Office of the Customs Financial

Enquiries, the cross-border trade of diamond and cocoa over Cote d'Ivoire's porous borders generates illicit funds that are primarily laundered via informal money services businesses and exchange houses. In addition to informal money service businesses, authorities believe criminal enterprises also use the formal banking system, cash couriers, and the used car and real-estate industries to launder funds. Cash earned by immigrant or migrant workers generally flows out of Cote d'Ivoire, going to extended families outside the region, although there is no evidence that such flows are tied to money laundering.

The banking sector is active, but because banking services were largely absent from the northern part of Côte d'Ivoire until the end of 2007, the public used informal money couriers, money transfer organizations similar to hawaladars and, increasingly, goods transportation companies to transfer funds domestically, as well as within the sub-region. The standard fee for informal money transfer services is approximately ten percent. There is no regulation of domestic informal value transfer systems. Informal remittance transfers from outside Cote d'Ivoire violate West African Central Bank (BCEAO) money transfer regulations.

Hizballah is present in Côte d'Ivoire and conducts fundraising activities, mostly among the large Lebanese expatriate community. The Ivorian government has taken no legal action to prevent the misuse of charitable and or other nonprofit entities that can be used as conduits for the financing of terrorism. Reportedly, the Ministry of Interior Security is addressing this problem.

There are no free trade zones in Cote d'Ivoire. However, in June 2008, the Export-Import Bank of India opened a $21 million line of credit for the Ivorian government to build a free trade zone for information technology and biotechnology in Grand Bassam. The Ivorian government has not yet chosen contractors for the project.

The Economic and Financial Police report an ongoing rise in financial crimes related to credit card theft and foreign bank account fraud. These include wire transfers of large sums of money primarily involving British and American account holders who are the victims of Internet-based advance fee scams. Cote d'Ivoire has no law specifically targeting Internet scams. The Ministry of Finance remains concerned by the high levels of tax fraud, particularly VAT tax fraud, by merchants.

Cote d'Ivoire has the largest bank network in the region. French financial interests account for the majority of retail and other banking and insurance services. The Ivorian banking law, enacted in 1990, prevents disclosure of client and ownership information, but does allow the banks to provide information to judicial authorities such as investigative magistrates. The law also permits the use of client and ownership information as evidence in legal proceedings or during criminal investigations. The Tax and Economic police can request information from the banks. Ivorian authorities recently amended the banking law, which now requires that banks be capitalized with $10 million and nonbank financial institutions (mortgage firms, insurance companies, etc.) with $5 million.

Originally, the penal code criminalized only money laundering related to drug trafficking, fraud, and arms trafficking. On November 29, 2005, the National Assembly adopted the l'Union Economique et Monetaire Ouest Africaine/West African Economic and Monetary Union (l'UEMOA/WAEMU), common law on money laundering. With this law, Cote d'Ivoire adopted the all-crimes approach to money laundering, making it a criminal offense regardless of the predicate offense.

The law focuses on the prevention of money laundering and also expands the definition to include the laundering of funds from all serious crimes. The law does not set a minimum threshold. It mandates standard "know your customer" requirements for banks and other financial institutions and establishes procedures and a suspicious transaction reporting obligation which covered institutions must follow to assist in the detection of money laundering. The law provides a legal basis for international cooperation. The new law includes both criminal and civil penalties, and permits the freezing and seizure of assets, which can be both instruments for and proceeds of crime. Legitimate businesses are among the assets that can be seized if used to launder money or support terrorism or other illegal

activities. Authorities cannot seize substitute assets, as assets can only be seized if there is a relationship between the assets and the offense. .

The money laundering law provides for the establishment of a financial intelligence unit (FIU) known as "Cellule Nationale de Traitement des Informations Financieres" (CENTIF) under the Minister of Finance. CENTIF became operational in January 2008. CENTIF can share information with other FIUs in l'UEMOA/WAEMU and with those of non-L'UEMOA/WAEMU countries on a reciprocal basis and with the permission of the Ministry of Finance, as long as those institutions keep the information confidential.

CENTIF is led by a group of six directors, detailed to the agency from the Finance Ministry, the Justice Ministry, police, customs, and the central bank/ CENTIF has 18 technical staff members, including financial analysts, an accountant, an attorney, an economist/statistician, and a computer network manager. It works with previously established investigative units such as the Centre de Recherche Financiere (CRF) at the Department of Customs and the Agence Nationale de Strategie et d'Intelligence (ANSI) at the presidency. The CRF and the ANSI continue to investigate fiscal and customs fraud and counterfeiting. The Economic and Financial police, the criminal police unit (Police Judiciaire), the Department of Territorial Surveillance, the CRF and ANSI all are responsible for investigating financial crimes, including money laundering and terrorist financing. Since its inception, CENTIF has received approximately 20 suspicious activity reports (the majority of them submitted by banks) and has forwarded two cases to prosecutors. To date, no arrests or convictions have resulted. CENTIF has also received three information requests. Although CENTIF has blocked funds, such action has proved counterproductive. Ivorian law allows funds to be blocked for a maximum of 48 hours, unless prosecution of a crime commences. In cases in which action does not take place within 48 hours, the holder of the account becomes aware that he or she is under suspicion and is likely to move the funds elsewhere. CENTIF's greatest deficiencies relate to a lack of funding and the need for training—both CENTIF's own employees as well as for prosecutors.

The FIU participates in the newly-formed National Committee, an interministerial committee dedicated to building effectiveness in the anti-money laundering/counterterrorist financing (AML/CTF) regime. The Committee has met seven times and developed a National Strategy and Action Plan for combating money laundering and terrorist financing. The Committee is working with the FIU on training initiatives and has participated in CENTIF's FIU orientation seminar.

The Ministry of Finance, the BCEAO, and the West African Banking Commission, headquartered in Cote d'Ivoire, supervise and examine banking compliance with AML/CTF laws and regulations. All Ivorian financial institutions must maintain customer identification and transaction records for ten years. Additionally in all BCEAO member countries, banking officials must report all deposits over CFA 5,000,000 (approximately $10,000) to the BCEAO, along with customer identification information. Law enforcement authorities can request access to these records to investigate financial crimes through a public prosecutor. In 2008, there were no arrests or prosecutions for money laundering or terrorist financing.

Legislation requires financial institutions to retain records of all "significant transactions," which are transactions with a minimum value of CFA 50,000,000 (approximately $100,000) for known customers, for ten years. New money laundering controls apply to nonbank financial institutions such as exchange houses, stock brokerage firms, insurance companies, casinos, cash couriers, national lotteries, nongovernment organizations, travel agencies, art dealers, gem dealers, accountants, attorneys, and real estate agents. The law also imposes certain customer identification and record maintenance requirements on casinos and exchange houses. The tax office (Ministry of Finance) supervises these entities. All Ivorian financial institutions, nonfinancial businesses, and professions subject to the scope of the money laundering law are required to report suspicious transactions. The

Ivorian banking code protects reporting individuals. Their identities are not divulged with respect to cooperation with law enforcement authorities.

Cote d'Ivoire monitors and limits the international transport of currency and monetary instruments under L'UEMOA/WAEMU administrative regulation R/09/98/CM/L'UEMOA/WAEMU; it does not have additional domestic laws or regulations. When traveling to another l'UEMOA/WAEMU country, Ivorian and expatriate residents must declare the amount of currency being carried out of the country. When traveling to a destination other than another l'UEMOA/WAEMU country, Ivorian and expatriate residents are prohibited from carrying an amount of currency greater than the equivalent of 500,000 CFA francs (approximately $1,000) for tourists, and two million CFA francs (approximately $4,000) for business operators, without prior approval from the Department of External Finance of the Ministry of Economy and Finance. If additional amounts are approved, they must be in the form of travelers' checks.

Cote d'Ivoire does not have a specific law that criminalizes terrorist financing, as required under UNSCR 1373, although financing of all "serious crimes" falls under the domain of the law. Until the passage of the 2005 money laundering law, the Government of Cote d'Ivoire (GOCI) relied on several l'UEMOA/WAEMU directives on terrorist financing, which provided a legal basis for administrative action by the GOCI to implement the asset freeze provisions of UNSCR 1373. The BCEAO and the government report that they promptly circulate to all financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's Consolidated List and those on the list of Specially Designated Global Terrorists designated by the U.S. pursuant to Executive Order 13224. To date, no assets related to terrorist entities or individuals have been discovered, frozen or seized.

The GOCI participates in the Intergovernmental Group for Action against Money Laundering (GIABA) based in Dakar, which is the Financial Action Task Force-style regional body (FSRB) for West Africa. GIABA has scheduled a mutual evaluation for Cote d'Ivoire for November 2009. Other than the authority granted to CENTIF by the AML law, the GOCI has neither adopted laws nor promulgated regulations that specifically allow for the exchange of records with the United States on money laundering and terrorist financing.

There are no laws or regulations that specifically permit the allow the exchange of records with United States on money laundering and terrorist financing, other than the authority granted to CENTIF by the AML law. However, Cote d'Ivoire has demonstrated a willingness to cooperate with the United States in investigating financial or other crimes. For example, in a 2007 case, a prominent American government official based in the UK was defrauded by a party based in Cote d'Ivoire who was using the individual's credit card information to purchase expensive medical equipment and ship it to Cote d'Ivoire. While the perpetrator(s) were not apprehended, Ivorian authorities worked cooperatively with U.S. law enforcement.

Cote d'Ivoire is a party to the UN Convention for the Suppression of the Financing of Terrorism and the 1988 UN Drug Convention. The GOCI has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. Cote d'Ivoire is ranked 151 out of 180 countries in Transparency International's 2008 Corruption Perceptions Index.

The Government of Cote d'Ivoire should specifically criminalize terrorist financing. The Ministry of Finance should continue to work to build capacity at CENTIF to maximize effectiveness in FIU functions, especially analysis, outreach and information sharing. CENTIF should work toward becoming a member of the Egmont Group. The GOCI's law enforcement and customs authorities need to implement measures to diminish smuggling, trade-based money laundering, and informal value transfer systems. Authorities should also take steps to halt the spread of corruption that permeates both commerce and government and facilitates the continued growth of the underground economy and

money laundering. Cote d'Ivoire should become a party to the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Cyprus

Cyprus has been divided since the Turkish military intervention of 1974, following an unsuccessful coup d'etat directed from Greece. Since then, the Republic of Cyprus (ROC) has controlled the southern two-thirds of the country, while a Turkish Cypriot administration calling itself the "Turkish Republic of Northern Cyprus (TRNC)" controls the northern part. Only Turkey recognizes the "TRNC." The U.S. Government recognizes only the Republic of Cyprus. This report primarily discusses the area controlled by the ROC but also includes a separate section on the area administered by Turkish Cypriots.

Cyprus is a major regional financial center with a robust financial services industry and a significant amount of nonresident businesses. Although Cyprus has made progress from its days as an offshore haven for tax evasion, money laundering and other types of criminal financial activity, Cyprus remains vulnerable to significant money laundering and illicit finance activities. Simple financial crime such as fraud and tax evasion, along with narcotics-trafficking and proceeds from organized crime are the major sources of illicit proceeds laundered in Cyprus.

A number of factors have contributed to the development of Cyprus as a financial center: the island's central location; a preferential tax regime; double tax treaties with 40 countries (including the United States, several European Union (EU) nations, and former Soviet Union nations); a labor force well trained in legal and accounting skills; a sophisticated telecommunications infrastructure; and EU membership. However, these same factors also make Cyprus attractive to illicit actors seeking access to European markets or desiring to launder criminal proceeds. Cyprus' historic ties to organized criminal elements and large number of shell companies—which may be used by criminals and proliferators as fronts to facilitate illegal activity—also may attract illicit financiers.

Cyprus currently hosts a total of 44 banks, 17 of which are incorporated locally. The remaining 27 banks are branches of foreign-incorporated banks and conduct their operations mainly with nonresidents. At the end of October 2008, the cumulative assets of all banks are €109 billion (approximately $147,150,000,000). Under the EU's "single passport" policy, banks licensed by competent authorities in EU countries may establish branches in Cyprus or provide banking services on a cross-border basis without obtaining a license from the Central Bank of Cyprus. By the end of 2008, nine foreign banks were operating branches in Cyprus under this arrangement.

Cyprus hosts seven licensed money transfer companies, 65 investment firms, two management firms handling "undertakings for collective investment in transferable securities" (UCITS), 43 licensed insurance companies, 400 licensed real estate agents, 2,496 registered accountants, 1,820 practicing lawyers, and approximately 118 cooperative credit institutions, controlling about 32 percent of total deposits. Stricter EU requirements on credit institutions have pushed cooperative credit institutions to merge on a large scale since 2004. Their number has declined from 359 to the current 118 in less than four years, and authorities expect this trend to continue.

In recent years, Cyprus has introduced tax and legislative changes effectively abolishing all legal and substantive distinctions between domestic and offshore companies. All Cypriot companies now pay taxes at a uniform rate of 10 percent, irrespective of the permanent residence of their owners or whether they do business internationally or in Cyprus. Cyprus has lifted the prohibition from doing business domestically and companies formerly classified as offshore are now free to engage in business locally. In March 2007, Cyprus withdrew from the Offshore Group of Banking Supervisors. By removing any distinction between resident and nonresident or on-shore and offshore companies, the same disclosure, reporting, tax and other laws and regulations apply equally to all registered

companies. Despite these stricter standards, few of the estimated 54,000 nonresident companies established in Cyprus as of 2006 have taken themselves off the company register, and the number of new nonresident companies registering in Cyprus continues to increase as a result of the low tax rate and high service quality. The high number of nonresident businesses raises concern about money laundering due to difficulties in monitoring their activities.

The Prevention and Suppression of Money Laundering Activities Law criminalizes all money laundering; establishes a customer identification requirement and obligations for suspicious transaction reporting; provides for the confiscation of proceeds from serious crimes; and codifies the actions that banks, nonbank financial institutions, and obligated nonfinancial businesses must take. The definition of predicate offense is any criminal offense punishable by a prison term exceeding one year. Money laundering is an autonomous crime in Cyprus. Cypriot AML legislation addresses government corruption, provides for the sharing of assets with other governments, and facilitates the exchange of financial information with other FIUs.

Due diligence and reporting requirements extend to auditors, tax advisors, accountants, and, in certain cases, attorneys, real estate agents, and dealers in precious stones and gems. The Institute of Certified Public Accountants of Cyprus—the designated supervisory authority for auditors and accountants in Cyprus—has publicized strict "know your customer (KYC)" regulations and has outsourced its supervisory oversight function to the UK's Association of Chartered Certified Accountants). The Cyprus Bar Association, which regulates lawyers, also has strict KYC regulations. Cypriot authorities reportedly have full access to information concerning the beneficial owners of every company registered in Cyprus. This includes companies doing business abroad and companies with foreign beneficial owners and shareholders. However, regulatory oversight of entities such as lawyers and accountants, who are involved in corporate registration and the collection of beneficial ownership information, remains low. This lack of oversight could complicate the ability of authorities to access beneficial ownership information if such information is not collected at the time of registration and can create a permissive environment for beneficial owners of shell companies who may use these firms to conceal illicit activities. The FIU can instruct banks, financial institutions and other obligated entities to delay or prevent execution of customers' transactions. Casinos and Internet gaming sites are not permitted, although sports betting halls are allowed.

ROC law requires all persons entering or leaving Cyprus to declare all Cypriot or foreign currency and gold bullion worth €12,500 (approximately $16,875) or more. The Central Bank has the authority to revise this amount. On June 15, 2007, EU Directive 1889/2005 went into effect regulating cash movements of currency worth €10,000 (approximately $13,500) or more for travelers entering Cyprus from countries outside the EU.

On December 13, 2007, Cyprus passed legislation entitled "Law for the Prevention and Suppression of Money Laundering Activities," (LPSMLA) which came into effect on January 1, 2008. This legislation consolidates and supersedes pre-existing legislation. It encompasses all recent recommendations of the Financial Action Task Force (FATF) and the recommendations made by the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), a FATF-style regional body (FSRB), at its mutual evaluation in 2006. The LPSMLA provides much stricter administrative fines for noncompliance, i.e., from €5,130 (approximately $6,925) to €200,000 (approximately $270,000), and generally raises Cyprus' AML standards.

The LPSMLA also addresses enhanced due diligence, extending coverage of "politically-exposed persons" (PEPs), cross-border transactions, and transactions with customers not physically present or acting on behalf of third parties. The law introduces simplified due diligence for certain persons or entities deemed to be low-risk, as well as requirements for the Unit for Combating Money Laundering (MOKAS), the Cypriot FIU, and other supervisory authorities to collect statistical data. MOKAS must

provide banks and other obligated entities with feedback in response to any suspicious transaction report (STR) submission.

Article 59 of the LPSMLA specifies the specific supervisory authorities for the various types of financial businesses, as well as other types of business activities. It also strengthens enforcement by expressly stipulating that directives issued by supervisory authorities are binding and obligatory, and by describing the range of possible enforcement measures, including requiring specific remedial action, imposing increased fines, and revoking the license of the supervised person or entity. Articles 61 and 62 describe the method and timeline for applying customer due diligence and identification procedures, while Article 64 refers to enhanced due diligence. Article 70 requires covered entities to notify the FIU before they carry out transactions that they know or suspect to be related to money laundering or terrorist financing. Furthermore, Article 49 provides an exception from the restriction on the disclosure of information, allowing the exchange of information between professionals belonging to the same group of companies.

While the recent AML law addresses many of the previously identified gaps in the Cyprus' AML/CTF regime, the effectiveness of these measures is unknown, as some provisions have not been fully implemented or tested through the detection, investigation and prosecution of money laundering cases.

Four authorities regulate and supervise financial institutions in Cyprus: the Central Bank of Cyprus, responsible for supervising locally incorporated banks and money transfer businesses; the Cooperative Societies Supervision and Development Authority (CSSDA), supervising cooperative credit institutions; the Superintendent for Insurance Control; and the Cyprus Securities and Exchange Commission (CSEC). Three entities act as regulators for designated nonfinancial businesses and professions (DNFBPs): the Council of the Bar Association supervises attorneys; the Institute of Certified Public Accountants supervises accountants; and the financial intelligence unit (FIU) supervises real estate agents and dealers in precious metals and stones. The supervisory authorities may impose administrative sanctions if the legal entities or persons they supervise fail to meet their obligations as prescribed in Cyprus' anti-money laundering (AML) laws and regulations.

In recent years the Central Bank has introduced directives aimed at strengthening AML vigilance in the banking sector. Among other requirements, banks must ascertain the identities of the natural persons who are the "principal/ultimate" beneficial owners of all legal entities; adhere to the October 2001 paper of the Basel Committee on Banking Supervision on "Customer Due Diligence for Banks"; and pay special attention to business relationships and transactions involving persons from jurisdictions identified by the FATF as deficient in their AML regime, particularly concerning counterterrorist financing. The definition of beneficial owner under Article 2 (b) of the LPSMLA is "the natural person(s), who is the beneficiary of or exercises control over 10 percent or more of the property of a legal arrangement or entity."

In April 2008, shortly after passage of the LPSMLA, the Central Bank issued a revised "Directive to Banks for the Prevention of Money Laundering and Terrorist Financing." Among other provisions, the new Directive assigns responsibility on all levels of bank management, including senior managers, for ensuring compliance and implementation; imposes additional duties on bank compliance officers; and specifies additional high-risk situations.

All banks must report to the Central Bank on a monthly basis individual cash deposits in any currency exceeding €10,000 (approximately $13,500). Bank employees must report all suspicious transactions to the bank's compliance officer, who determines whether to forward a report to the Cypriot FIU for investigation. Banks retain reports not forwarded to the FIU, which the Central Bank audits as part of its regular on-site examinations. Banks also must file monthly reports with the Central Bank indicating the total number of STRs submitted to the compliance officer and the number forwarded by the compliance officer to the FIU. Bank officials may be held personally liable if their institutions launder money. Cypriot law partially protects reporting individuals with respect to their cooperation with law

enforcement but does not clearly absolve a reporting institution or its personnel from complete criminal or civil liability. Banks must retain client identification data, transaction records, and business correspondence for five years.

Central Bank money laundering directives place additional obligations on banks, including requirements on customer acceptance policy and the updating of customers' identification data and business profiles. Banks must have computerized risk management systems to verify whether a customer is a PEP. They must also provide full details on any customer sending an electronic transfer in excess of €1,000 (approximately $1,350), and have adequate management information systems for on-line monitoring of customers' accounts and transactions. Cypriot banks typically use electronic risk management systems to target transactions involving high-risk countries, as well as high-risk customers. Since January 1, 2007, Cyprus has been implementing EU Directive 1781/2006 ("Information on the Payer Accompanying Transfers of Funds"), which requires full disclosure of details for electronic fund transfers in excess of €1,000 (approximately $1,350.

The Central Bank also requires compliance officers to file annual reports outlining measures taken to prevent money laundering and to comply with its directives and relevant laws. In addition, the Central Bank has the authority to conduct unannounced inspections of bank compliance records. In July 2002, the U.S. Internal Revenue Service (IRS) officially approved Cyprus' "know-your-customer" rules, which form the basic part of Cyprus' AML system. This approval allows banks in Cyprus that acquire United States securities on behalf of their customers to enter into a "withholding agreement" with the IRS and become qualified intermediaries.

A draft law, expected to pass in early 2009, will regulate trust and company service providers (other than accountants and lawyers), bringing them under the supervisory authority of the Central Bank. As soon as this law goes into effect, the supervisory authorities will issue revised directives.

In October 2006, the IMF released a detailed assessment of the "Observance of Standards and Codes for Banking Supervision, Insurance Supervision and Securities Regulation." The report notes that the CSEC is legally unable to cooperate with foreign regulators if the CSEC does not have a direct interest, and that the CSEC has difficulty obtaining information regarding the beneficial owners of Cypriot-registered companies. The CSEC drafted amending legislation to resolve these issues, expected to pass in 2008, but now anticipated in early 2009. In the meantime, an amendment to the Market Abuse Law, passed in late 2007, enables the CSEC to share information with other competent authorities, as necessary. The IMF report also notes that commitments emerging from EU accession had "placed stress on the skills and resources" of the staff of the CSSDA and of the Insurance Superintendent.

The Prevention and Suppression of Money Laundering Activities Law mandates the establishment of MOKAS, the Cypriot FIU, and authorizes criminal (but not civil) seizure and forfeiture of assets. MOKAS is responsible for receiving and analyzing STRs and for conducting money laundering investigations. A representative of the Attorney General's Office heads the unit. All banks and nonbank financial institutions, insurance companies, the stock exchange, cooperative banks, lawyers, accountants, and other financial intermediaries must report suspicious transactions to MOKAS. Sustained efforts by the Central Bank and MOKAS to strengthen reporting have resulted in a significant increase in the number of filed STRs. Between January 1 and December 18, 2008, MOKAS received 242 STRs. In the same interval, MOKAS received 321 information requests from foreign FIUs, other foreign authorities, and INTERPOL. MOKAS cooperates closely with the U.S. in money laundering investigations.

MOKAS evaluates evidence generated by its member agencies and other sources to determine whether an investigation is necessary. MOKAS has the power to administratively suspend financial transactions for an unspecified period of time. MOKAS also has the power to apply for freezing or restraint orders affecting any kind of property at a preliminary stage of an investigation. MOKAS has

issued several warning notices, based on its own analysis, identifying possible trends in criminal financial activity. These notices have resulted in the closure of dormant bank accounts. MOKAS conducts AML training for Cypriot police officers, bankers, accountants, and other financial professionals.

During the interval from January 1 through December 18, 2008, MOKAS opened 563 cases and closed 195. Since 2000, there have been 20 prosecutions for money laundering, seven of which took place in 2008. Of the 20 prosecutions, 11 have resulted in convictions. In 2008, MOKAS issued three confiscation orders for a total of approximately €70,000 (approximately $94,500). A number of other cases are pending. Despite the size of the financial sector and the seemingly comprehensive nature of the AML/CTF legislative regime, the number of reports, investigations and convictions of money laundering cases in Cyprus remains surprisingly low. Furthermore, suspicious transaction reporting from the nonfinancial sector, including lawyers and accountants, also remains low.

Sections four and eight of Ratification Law 29 (III) of 2001 criminalize terrorist financing. The implementing legislation amends the AML law to criminalize the collection of funds in the knowledge that they would be used by terrorists or terrorist groups for violent acts. The parliament passed an amendment to the implementing legislation in July 2005 eliminating a loophole that had inadvertently excused Cypriot nationals operating in Cyprus from prosecution for terrorist finance offenses. The LPSMLA criminalizes the general collection of funds with the knowledge that terrorists or terrorist groups would use them for any purpose (i.e., not just for violent acts); and explicitly covers terrorist finance (although already considered a predicate offense under existing legislation). MOKAS routinely asks banks to check their records for any transactions by any person or organization designated by foreign FIUs or the U.S. Treasury Department as a terrorist or terrorist organization.

Under a standing instruction, the Central Bank automatically issues a "search and freeze" order for accounts matching the name of any entity or group designated as a terrorist or terrorist organization by the UN 1267 Sanctions Committee or the EU 931Working Party, which replaced the previous informal EU "clearinghouse" with more formal mechanisms. If a financial institution finds matching accounts, it will immediately freeze the accounts and inform the Central Bank. As of November 2008, no bank has reported holding a matching account. When FIUs or governments—not the UN or the EU 931 Working Party—designate and circulate the names of suspected terrorists, MOKAS has the authority to block funds and contact commercial banks directly to investigate. To date, none of these checks have revealed anything suspicious. The lawyers' and accountants' associations cooperate closely with MOKAS and the Central Bank. Cyprus cooperates with the United States to investigate terrorist financing. MOKAS reports no terrorist assets have been found in Cyprus to date and thus there have been no terrorist financing prosecutions or freezing of terrorist assets. In 2006, there was one investigation for terrorist financing involving four persons.

Cyprus believes that its existing legal structure is adequate to address money laundering through alternative remittance systems such as hawala. Cypriot authorities maintain there is no evidence that alternative remittance systems such as hawala operate in Cyprus. Cyprus licenses charitable organizations, which must submit copies of their organizing documents and annual statements of account to the government. The majority of charities registered in Cyprus are reportedly domestic organizations.

Cyprus is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Cyprus has signed, but not yet ratified, the UN Convention against Corruption. Cyprus is a member of MONEYVAL. MOKAS is a member of the Egmont Group and has signed memoranda of understanding (MOUs) with 17 FIUs, although Cypriot law allows MOKAS to share information with other FIUs without benefit of an MOU. A mutual legal assistance treaty between Cyprus and the United States entered into force September 18, 2002.

The Government of Cyprus has put in place a comprehensive anti-money laundering/counterterrorist financing regime, which it continues to upgrade. Cyprus should ensure not only the passage, but also the full implementation, of the two laws that will regulate trusts and company service providers, and provide the CSEC with the ability to obtain necessary information and share information both domestically and internationally. The GOC should provide a clear safe harbor to individuals who cooperate with law enforcement. Cyprus should provide adequate resources and capacity to the CSSDA and the Insurance Superintendent. Cyprus should also increase regulatory oversight of designated nonfinancial businesses and professions (DNFBPs) including lawyers and accountants. The ROC should ensure it is able to implement the law criminalizing the collection of funds with the knowledge they will be used by terrorists or terrorist groups for any purpose, not only to commit terrorist or violent acts. Cyprus should consider enacting provisions that allow for civil forfeiture of assets. Cyprus should ratify the UN Convention against Corruption.

Area Administered by Turkish Cypriots

The Turkish Cypriot community continues to lack the legal and institutional framework necessary to provide effective protection against the risks of money laundering, although significant progress has been made over the last year. There are currently 24 domestic banks in the area administered by Turkish Cypriots and Internet banking is available. The offshore sector consists of 14 banks and 34 companies. The offshore banks may not conduct business with residents of the area administered by Turkish Cypriots and may not deal in cash. The "Central Bank" audits the offshore entities, which must submit an annual report on their activities. Under revised laws passed in 2008, the "Central Bank" took over the regulation and licensing of offshore banks from the "Ministry of Finance." The new law permits only banks previously licensed by Organization for Economic Co-operation and Development (OECD)-member nations or having "friendly relations" with "TRNC" to operate an offshore branch in northern Cyprus.

It is thought the 23 essentially unregulated and primarily Turkish-mainland owned casinos and the 14 offshore banks are the primary vehicles through which money laundering occurs. Casino licenses are fairly easy to obtain, and background checks on applicants are minimal. A significant portion of the funds generated by these casinos reportedly changes hands in Turkey without ever entering the Turkish Cypriot banking system, and there are few safeguards to prevent the large-scale transfer of cash to Turkey. Recent years have seen a large increase in the number of sport betting halls, which are licensed by the "Office of the Prime Minister." There are currently five companies operating in this sector, with approximately 30 outlets. Four of the companies also accept bets over the Internet. Turkish Cypriot authorities deported one prominent Turkish organized crime figure, Yasar Oz, following a December 19, 2006 shootout at the Grand Ruby Casino that left two dead. As a result of this incident, the Turkish Cypriot authorities arrested seven individuals, closed the Grand Ruby and Denizkizi Casinos and deported much of their staffs. Nevertheless, several other casinos are still believed to have significant links to organized crime groups in Turkey. Casinos fall under the purview of the AML law passed in 2008. A draft law, expected to be passed in January 2009, is designed to tighten the licensing and regulation of casinos.

Another area of concern is the approximately five hundred "finance institutions" that extend credit and give loans. Although they must register with the "Office of the Registrar of Companies," they remain unregulated. Some of these companies are owned by banks and others by auto dealers.

The fact that the "TRNC" is recognized only by Turkey limits the ability of Turkish Cypriot authorities to receive training or funding from international organizations with experience in combating money laundering. The Turkish Cypriot community is not part of any FSRB and thus is not subject to normal peer evaluations. In 2007, FATF conducted an informal review and found numerous shortcomings in AML laws and regulations as well as insufficient resources devoted to the effort. Turkish Cypriot officials objected to the conclusions. After including the northern part of Cyprus as an

area of concern for money laundering in February 2008, FATF found "significant progress" had been made by its October 2008 meeting.

The offshore banking sector remains a concern. In August 2004, the U.S. Department of the Treasury's FinCEN, pursuant to Section 311 of the USA PATRIOT Act, found First Merchant Bank to be of primary money laundering concern based on a number of factors. These factors include that the bank is licensed as an offshore bank in a jurisdiction with inadequate AML controls, particularly those applicable to its offshore sector; and it is involved in the marketing and sale of fraudulent financial products and services. Other factors point to its use as a conduit for the laundering of fraudulently obtained funds and its apparent use to launder criminal proceeds by individuals with links to organized crime who own, control, and operate First Merchant Bank. In December 2006, the Turkish Cypriot administration ordered First Merchant Bank to cease its operations due to violations of the Turkish Cypriot "Offshore Banking Law." The bank is now only permitted to perform activities associated with closing the bank such as the payment and collection of outstanding debts.

Turkish Cypriot authorities have begun taking steps to address the risk of financial crime, including enacting an anti-money laundering law ("AMLL") for the area. The law aims to reduce the number of cash transactions in the area administered by Turkish Cypriots as well as improve the tracking of any transactions above €10,000 (approximately $13,500). Under the "AMLL," banks must report to the "Central Bank" and the "Money and Exchange Bureau" any electronic transfers of funds in excess of $100,000. Such reports must include information identifying the person transferring the money, the source of the money, and its destination. Under the new law, banks, nonbank financial institutions, and foreign exchange dealers must report all currency transactions over €10,000 (approximately $13,500) and suspicious transactions in any amount to the "Money and Exchange Bureau" which deals with AML at the "Ministry of Finance." Banks must follow a know-your-customer policy and require customer identification. Banks also must submit STRs to a five-member "Anti-Money Laundering Committee (AMLC)" which decides whether to refer suspicious cases to the "police" and the "attorney general's office" for further investigation. The five-member committee is composed of representatives of the "police," "customs," the "Central Bank," and the "Ministry of Finance."

In 2005, the "AMLC," which had been largely dormant for several years, began meeting on a regular basis and encouraging banks to meet their obligations to file STRs. The committee has referred several cases of possible money laundering to law enforcement for further investigation, but no cases have been brought to court and no individuals have been charged. There have been no successful prosecutions of individuals for money laundering, although one foreign bank owner suspected of having ties to organized crime was successfully extradited. There are significant concerns that law enforcement and judicial authorities lack the technical skills needed to investigate and prosecute financial crimes. The "AMLC" also complains that since foreign jurisdictions will not cooperate with it by providing evidence or appearing to testify, the authorities have difficulty presenting cases to their court system.

The "AMLL" requires individuals entering the area administered by Turkish Cypriots to declare cash over $10,000 and prohibits individuals leaving the area administered by Turkish Cypriots from transporting more than $10,000 in currency. However, "Central Bank" officials note that this law is difficult to enforce. This is particularly true given the large volume of travelers to and from Turkey, especially since Turkish Cypriot authorities relaxed restrictions that limited travel across the UN-patrolled buffer zone. There is also a relatively large British population in the area administered by Turkish Cypriots and a significant number of British tourists. As a result, an informal currency exchange market has developed.

The Turkish Cypriot "AMLL" provides better banking regulations than were in force previously, but as an AML tool it is far from adequate, and without ongoing enforcement, cannot meet its objectives. A major weakness continues to be the many casinos, where a lack of resources and expertise leave the

area essentially unregulated and therefore especially vulnerable to money laundering abuse. The largely unregulated finance institutions, currency exchange houses, and offshore banking sector are also of concern. The Turkish Cypriot authorities should move quickly to establish a strong, functioning "financial intelligence unit," and adopt and implement a strong licensing and regulatory environment for all obligated institutions, in particular casinos, money exchange houses, and entities in the offshore sector. Turkish Cypriot authorities should stringently enforce the cross-border currency declaration requirements. Turkish Cypriot authorities should take steps to enhance the expertise of members of the enforcement, regulatory, and financial communities with an objective of better regulatory guidance, more efficient STR reporting, better analysis of reports, and enhanced use of legal tools available for prosecutions.

Czech Republic

The Czech Republic is one of the most stable and prosperous of the post-Communist states of Central and Eastern Europe. However, the Czech Republic's central location in Europe and its relatively new status as a functional market economy have left it vulnerable to money laundering. While various forms of organized crime (narcotics-trafficking, trafficking in persons, fraud, counterfeit goods, embezzlement, and smuggling) remain the primary sources of laundered assets in the country, Czech officials and media outlets voice concern about the ability of extremist groups and terrorists to launder or remit money within the country. Domestic and foreign organized crime groups target Czech financial institutions for laundering activity, most commonly by means of financial transfers through the Czech Republic. Banks, casinos and other gaming establishments, investment companies, and real estate agencies have all been used to launder criminal proceeds. Currency exchanges in the capital and border regions are also considered to be a problem. For many years, the Czech Republic was a transfer country in the international illegal animal trade. In recent years, authorities have reported an increase in cases of animal smuggling and believe the Czech Republic is becoming a target for such activity. In the Czech Republic, animals reportedly come third on the list of smuggled goods after drugs and weapons. Last year, the authorities confiscated altogether 151 animals, mainly tortoises, songbirds and parrots.

The growth of the Czech Republic economy between 2000 and 2008 was supported by exports to the European Union (EU). However, despite the progressive development of modern payment techniques, the economy is still heavily cashed-based. Major sources of criminal proceeds include criminal offenses against property, insurance fraud, and credit fraud. Insurance fraud in the Czech Republic rose by 50 percent in the first quarter of 2008. The Czech Association of Insurance Companies (CAIC) says that one in five insurance claims is fraudulent. The most common type of fraud concerns car insurance and property damage claims. Connections between organized crime and money laundering have been observed mainly in relation to activities of foreign groups, in particular from the former Soviet republics, the Balkan region, and Asia. Criminal groups operating in the Czech Republic are mostly of foreign origin. They often enter the country by first opening various front companies, then receiving residency permits for employment in their own companies. Alternatively, immigrants often start business companies, which in many cases create the base for illegal migration, which subsequently creates a personnel base for criminal organizations. The Czech Republic is also vulnerable to other illicit financial activities conducted through credit and loan services, money remittances (particularly in connection with the Asian community), and illegal foreign exchange business.

The Government of the Czech Republic (GOCR) first criminalizes money laundering in September 1995 through additions to its Criminal Code. Although the Criminal Code does not explicitly mention money laundering, its provisions apply to financial transactions involving the proceeds of all serious crimes. A July 2002 amendment to the Criminal Code introduces a new independent offense called "Legalization of Proceeds from Crime." This offense has a wider scope than previous provisions and

enables prosecution for laundering one's own illegal proceeds (as opposed to those of other parties). The 2002 amendment also stipulates punishments of five to eight years imprisonment for the legalization of proceeds from all serious criminal activity and calls for the forfeiture of assets associated with money laundering. Section 252a, "Legalization of Proceeds from Criminal Activity," of the Criminal Code criminalizes money laundering.

The Czech anti-money laundering legislation became effective in July 1996. The Anti-Money Laundering (AML) Act (Act No. 61/1996, Measures Against Legalization of Proceeds from Criminal Activity) provides the general preventive AML framework. It has been amended eleven times. The latest amendment, Act No. 253/2008 came into force September 1, 2008. Act No. 253/2008 requires customers to verify their identities for all transactions exceeding 1,000 euros (approximately $1,400). The previous limit was 15,000 euros (approximately $21,000). For transactions above 15,000 euros (approximately $21,000), customers are required to provide more extensive information that includes details of the purpose and nature of the intended transaction. The new law also calls for more stringent controls of financial transactions involving politically exposed persons (PEPs) and their immediate family members. The law now requires a wide range of financial institutions, as well as attorneys, casinos, realtors, notaries, accountants, tax auditors, and entrepreneurs engaging in financial transactions, to report all suspicious transactions to the Ministry of Finance's financial intelligence unit (FIU), known as the Financial Analytical Unit (FAU). The institutions must all keep internal records of all transactions exceeding 1,000 euros (approximately $1,400). Although, in general, the customer identification procedures are mostly in place, full customer due diligence (CDD) requirements should be introduced in the AML Act with appropriate guidance.

The Czech Republic still has more than 2.6 million anonymous deposit passbooks containing 3.9 billion crowns (approximately $200,000,000). Due to ongoing criticism, the Czech Republic introduced legislation in 2000 prohibiting new anonymous passbook accounts. In 2002, the Act on Banks was amended to abolish all existing bearer passbooks by December 31, 2002. In principle, bearer passbooks will be completely phased out by 2012. While account holders can still withdraw money from the accounts for another few years, the accounts do not earn interest and cannot accept deposits. In 2007, approximately 350 million crowns (approximately $18,000,000) were withdrawn from these accounts.

Czech authorities require that financial institutions maintain transaction records for a period of ten years. Reporting requirements also apply to persons or entities seeking to enter the Czech Republic. Under the provisions of the AML Act, anyone entering or leaving the Czech Republic with more than 10,000 euros (approximately $14,000) in cash, traveler's checks, or other monetary instruments must make a declaration to customs officials, who are required to forward the information to the FAU. Similar reporting requirements apply to anyone seeking to mail the same amount in cash to or from the country. In practice, the effectiveness of these procedures is difficult to assess. As a result of the Czech Republic's December 2007 entry into the Schengen zone, all passport and customs stations on the borders are closed. Although the customs station at the Prague Airport remains operational, detecting the smuggling or transport of large sums of currency by train or highway is difficult.

The FAU was established in July 1996 as an administrative FIU under the umbrella of the Ministry of Finance. It has overall supervisory competence to ensure the implementation of the AML Act by all obliged entities. Since 1996, financial institutions have been required to report all suspicious transactions to the FAU. The FAU is authorized to cooperate with the Czech Intelligence Service (BIS) and Czech National Security Bureau (NBU) in addition to its ongoing cooperation with the Czech Police, Customs, and counterpart FIUs abroad.

The FAU is charged with reviewing cash transaction reports (CTRs) and suspicious transaction reports (STRs) filed by police agencies, financial, and other institutions. It is also charged with uncovering cases of tax evasion, a widespread problem in the Czech Republic. The FAU has neither the mandate

nor the capacity to initiate or conduct criminal investigations. The FAU's work covers only a relatively small segment of total financial activity within the Czech Republic. Since April 2006, the FAU has had the power to fine financial institutions that fail to report accounts or other assets belonging to individuals, organizations, or countries on which international sanctions have been imposed.

The number of STRs transmitted to the FAU decreased in 2007 after several years of rapid growth. There were 3,404 suspicious transactions reported in 2005, 3,480 in 2006, but only 2,048 in 2007. During the first five months of 2008, the FAU received 1,722 STRs. The number of inquiries evaluated and forwarded to law enforcement bodies also has decreased. In 2005, the FAU forwarded 208 reports to the police, 137 in 2006 and only 102 in 2007. During the first five months of 2008, the FAU forwarded 67 reports to the police.

Investigative responsibilities remain with the Czech National Police Unit for Combating Corruption and Financial Crimes (UOKFK) or other Czech National Police bodies. The UOKFK has primary responsibility for all financial crime, corruption and terrorist financing cases. Following the dissolution of the specialized Financial Police on January 1, 2007, the unit became the main law enforcement counterpart to the FAU. Following the abolition of the Financial Police, the UOKFK took over all of its ongoing cases, but the pace of investigations has slowed. The abolition of the Financial Police and the transfer of its cases to the UOKFK caused temporary difficulties in communication between the FAU and the Police. It is not clear whether every case transferred to law enforcement was investigated.

The Czech Republic saw its first convictions of individuals attempting to legalize proceeds from crime in 2004. In 2005, there were 23 alleged offenders prosecuted and three were convicted. In 2006, 33 were prosecuted, and five were convicted. In 2007, the Police investigated 32 cases, 13 of which are being prosecuted. As of November 2008, no data is available regarding the number of convictions. In the past, sentences have been low and generally consisted of suspended sentences or fines. A new Penal Code is likely to come into effect in 2009 and is expected to significantly increase penalties for financial crimes, including money laundering. An ongoing issue in criminal prosecutions is that law enforcement agencies must prove the assets in question were derived from criminal activity. The accused is not obligated to prove the property or assets were acquired legitimately.

While the institutional capacity to detect, investigate, and prosecute money laundering and financial offenses has increased in recent years, both the FAU and the police face staffing challenges. The Financial Action Task Force (FATF) and the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), a FATF-style regional body, have both emphasized the need for the Czech Republic to increase the FAU's staff. Despite numerous requests by the FAU for an increase in staffing, to date, the GOCR has not yet approved the FAU's request. Given the scope of its responsibilities, the FAU remains a relatively small organization. The police face even bigger challenges due to recent changes in police retirement rules and the perceived lack of political support for independent police work. Many senior and experienced police officers are reportedly leaving or are considering early retirement. These departures will affect not only the UOKFK, but the Organized Crime Unit and other critical police organizations as well. The dissolution of the Financial Police, which was created in 2004 and had a good track record of investigating and prosecuting money laundering and terrorist financing cases, has also had a negative impact on police work on financial crimes.

The Law on Implementation of International Sanctions that came into force in April 2006 also represents progress by the GOCR. Under this law, the Ministry of Finance has the authority to fine institutions for failure to report accounts or other assets belonging to individuals, organizations, or countries on which international sanctions have been imposed, or those not fulfilling other obligations

set by international regulations. Earlier laws restricting financial cooperation with the Taliban (2000) and Iraq (2005) were replaced by the Law on Implementation of International Sanctions.

Czech laws facilitate the seizure and forfeiture of bank accounts. A financial institution that reports a suspicious transaction has the authority to freeze the suspect account for up to 24 hours. However, for investigative purposes, this time limit can be extended to give the FAU sufficient time to investigate whether there is evidence of criminal activity. Currently, the FAU is authorized to freeze accounts for 72 hours. If sufficient evidence of criminal activity exists, the case is forwarded to UOKFK, which has another three days to gather the necessary evidence. If the UOKFK is able to gather enough evidence to start prosecution procedures, then the account can stay frozen for the duration of the investigation and prosecution. If, within the 72-hour time limit, the UOKFK fails to gather sufficient evidence to convince a judge to begin prosecution, the frozen funds must be released. These time limits do not apply to accounts owned by suspected terrorists and terrorist organizations, or by other individuals and organizations covered under the Law on Implementation of International Sanctions.

Although Czech law authorizes officials to use asset forfeiture, it is still not widely used. It was introduced into the criminal system in 2002 and allows judges, prosecutors, or the police (with the prosecutor's consent) to freeze an account or assets if evidence indicates the contents were used or will be used to commit a crime, or if the contents are proceeds of criminal activity. In urgent cases, the police can freeze the account without the previous consent of the prosecutor, but within 48 hours must inform the prosecutor, who then confirms the freeze or releases the funds. An amendment to the 2004 Law on the Administration of Asset Forfeiture in Criminal Procedure implements provisions and responsibilities addressing the administration and storage of seized property and appoints the police as administrators of seized assets.

A 2006 amendment to the Czech Criminal Procedure Code and Penal Code brings several positive changes to the asset forfeiture and seizure law. The law, as amended, now allows for the freezing and confiscation of the value of any asset (including immovable assets) and is not limited to property. These provisions allow the police and prosecutors to seize assets gained in illicit activity previously shielded by family members. The law allows for the seizure of substitute assets as well as equivalent assets not belonging to the criminal.

The National Drug Headquarters (NDH) cooperates with the UOKFK on drug-related cases. However, as a result of the abolition of the Financial Police the NDH conducts its basic financial investigations alone and, if needed, contacts the UOKFK. In 2007, the NDH confiscated the equivalent of approximately $165,000 in euros and CZK, and other assets worth CZK 1.92 million (approximately $106,700). For the first ten months of 2008, the figures are approximately $161,888 in CZK and euros, and other assets valued at CZK 1.72 million (approximately $95,556).

In November 2004, the Czech Government amended the Criminal Code and enacted new definitions for terrorist attacks and terrorist financing. The amendments impose a penalty of up to 15 years' imprisonment on those who support terrorists financially, materially, or by other means. On November 11, 2008, the lower house of the Czech Parliament passed a new penal code that will tighten the penalties for financing terrorism from the present 8-15 years to 12-20 years imprisonment. The code, however, must still be passed by the Senate and signed by the President before it can go into effect. In addition to reporting all suspicious transactions possibly linked to money laundering, concerned institutions are now required to report all transactions suspected of being tied to terrorist financing. An amendment to the AML law in 2000 requires financial institutions to freeze assets that belong to suspected terrorists and terrorist organizations on the UN 1267 Sanctions Committee consolidated list.

The GOCR adopted the National Action Plan for the Fight Against Terrorism for 2005-2007, subsequently updated for 2007-2009. This document covers topics such as police work and cooperation, protection of security interests, enhancement of security standards, and customs issues. The fight against terrorist financing is one of the major priorities contained in the plan.

Although the terrorist financing threat in the Czech Republic is considered to be modest, some law enforcement officials believe the presence of third-country remuneration networks operating in the country ("hawala" shops) could translate into a greater possibility of terrorist financing activities. The Czech Republic has specific laws criminalizing terrorist financing and legislation permitting rapid implementation of UN and EU financial sanctions, including action against accounts held by suspected terrorists or terrorist organizations. An informal interagency body called the Clearinghouse was established in 2002 under the FAU to streamline the collection of information from institutions and enhance cooperation and response to a terrorist threat. The Clearinghouse meets only in cases of necessity. The FAU is currently distributing lists of designated terrorists to relevant financial and governmental bodies. Czech authorities have been cooperative in the global effort to identify suspect terrorist accounts, and adoption of the Law on Implementation of International Sanctions has made their work easier. Several cases have been detected, and payments to suspected organizations were not permitted. In two cases sanctions had been imposed.

The Czech Republic has signed memoranda of understanding on information exchange with 23 countries, the most recent being Paraguay. The Czech Republic formalized an agreement with Europol in 2002. The FAU has been a member of the Egmont Group since 1997 and is authorized to cooperate and share information with all of its international counterparts, including those that are not part of the Egmont Group. Cooperation with foreign counterparts remains good. In 2005, the FAU received 130 assistance requests from foreign counterparts and sent 69 requests abroad. In 2006, it received 128 requests and sent out 77. In 2007, the FAU received 133 requests and sent out 66.

The Czech Republic participates in MONEYVAL. The most recent mutual evaluation of the Czech Republic was conducted by MONEVAL in 2005. The mutual evaluation report was adopted by MONEYVAL at its plenary meeting in September 2007. The Czech Republic is a party to the 1988 UN Drug Convention and the UN Convention for the Suppression of the Financing of Terrorism. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

The United States and the Czech Republic have a Mutual Legal Assistance Treaty (MLAT), which entered into force on May 7, 2000. In May 2006, the United States and the Czech Republic signed a supplemental MLAT, which was ratified in 2007, but has not yet come into force.

The Government of the Czech Republic has made progress in its efforts to strengthen its anti-money laundering regime. However, the GOCR should strengthen its incomplete legal framework on seizure and confiscation and take steps to resolve its FIU and police resource problems. The GOCR also should increase staffing and resources for the FAU and national police so these agencies can effectively implement and enforce the anti-money laundering/counterterrorist financing measures under their charge. To successfully implement its risk-based approach, the GOCR must adopt and put in place a comprehensive CDD program and ensure that all obligated entities have the capacity and guidance to apply it. The GOCR also should ratify the UN Convention against Transnational Organized Crime and UN Convention against Corruption.

Dominican Republic

As a major transit country for drug trafficking, the Dominican Republic remains vulnerable to money laundering. Financial institutions in the Dominican Republic engage in currency transactions involving international narcotics trafficking proceeds that include significant amounts of U.S. currency or currency derived from illegal drug sales in the United States. The smuggling of bulk cash by couriers and the use of wire transfer remittances are the primary methods for moving illicit funds from the United States into the Dominican Republic. Once in the Dominican Republic, currency exchange houses, money remittance companies, real estate and construction companies, and casinos facilitate the laundering of these illicit funds. The lack of a viable financial intelligence unit and the proposed

creation of an offshore financial center exacerbate the Dominican Republic's vulnerability to money laundering.

Money laundering in the Dominican Republic is criminalized under Act 17 of 1995 (the 1995 Narcotics Law) and Law No. 72-02 of 2002. Under these laws, the predicate offenses for money laundering include illegal drug activity, trafficking in human beings or human organs, arms trafficking, kidnapping, extortion related to recordings and electronic tapes, theft of vehicles, counterfeiting of currency, fraud against the state, embezzlement, and extortion and bribery related to drug trafficking. Law 183-02 also imposes financial penalties on institutions that engage in money laundering, and the Government of the Dominican Republic (GODR) is in the process of amending the law to add a parallel structure of criminal penalties.

The 1995 Narcotics Law allows preventive seizures and criminal forfeiture of drug-related assets, and authorizes international cooperation in forfeiture cases. Law No. 78-03 permits the seizure, conservation and administration of assets that are the product or instrument of criminal acts pending judgment and sentencing. However, there is a lack of regulations to implement the legislation that led to ineffective asset inventory and management. There is a pending amendment to Law No. 78-03 recently introduced by the GODR Attorney General's office. If approved, this amendment will greatly improve the administration of seized, confiscated, or abandoned properties and will also significantly reduce the time period that seized property must be held prior to forfeiture. Assets Laundering Law 72-02 applies to seized assets. While narcotics-related investigations have been initiated under the 1995 Narcotics Law, and substantial currency and other assets have been confiscated, there have been only four successful money laundering prosecutions under this law. None were reported for 2008.

Under Law No. 72-02 and Decree No. 288-1996, numerous financial and nonfinancial institutions are subject to anti-money laundering provisions. Obligated entities include banks, currency exchange houses, stockbrokers, securities brokers, the Central Bank, cashers of checks or other types of negotiable instruments, issuers/sellers/cashers of travelers checks or money orders, credit and debit card companies, remittance companies, offshore financial service providers, casinos, real estate agents, automobile dealerships, insurance companies, and certain commercial entities such as those dealing in firearms, metals, archeological artifacts, jewelry, boats, and airplanes. The law mandates that these entities must report suspicious transactions as well as all currency transactions exceeding $10,000, and maintain records for a minimum of five years. Moreover, the legislation requires individuals to declare cross-border movements of currency that are equal to or greater than the equivalent of $10,000 in domestic or foreign currency.

In August 2006, the Dominican Republic Attorney General created the Money Laundering Unit to actively pursue financial crimes and money laundering investigations to aid in prosecutors' ability to obtain money laundering convictions. Since 2006, there have been 25 investigations and seven cases brought to court, one of which is the Banco Intercontinental (BANINTER) case.

The 2003 collapse of BANINTER revealed 14 years of double-bookkeeping designed to hide "sweetheart" loans, embezzlement, and money laundering. Subsequent state reimbursement of depositors resulted in costs of approximately $2.3 billion. With the fraud-based collapse of Banco Mercantil and Banco Nacional de Credito (BANCREDITO) that same year, total bank fraud-based losses to the Dominican government approached $3 billion in 2003. These frauds gutted the Dominican economy, almost tripled national indebtedness, and caused a massive devaluation of the Dominican peso. The GODR negotiated an International Monetary Fund (IMF) standby loan in August 2003 to help cover the costs of the failures. The IMF insisted on extensive changes in laws and procedures to improve banking supervision. Though legislative changes have been made, full implementation of IMF requirements lags.

In the BANINTER case, the bank's president and vice- president were convicted and sentenced for violations of banking and monetary laws, although both were acquitted of money laundering. A

Dominican economist and entrepreneur, a U.S. citizen, was convicted of criminal money laundering in connection with the collapse and sentenced to ten years in prison. In November 2008, the Dominican Supreme Court upheld the convictions in the BANCREDITO case, although none of the convictions were for money laundering. While these convictions were criticized by civil society, the media, and jurists as internally inconsistent, reportedly, they nevertheless serve as a significant challenge to impunity for the country's elite.

In 1997, the Dominican Republic established the Unidad de Inteligencia Financiera (UIF) as the country's financial intelligence unit (FIU) with the responsibility of receiving financial disclosures and suspicious transaction reports (STRs) from reporting entities in the financial sector. In 2002, Law 72-02 created the Unidad de Análisis Financiero (Financial Analysis Unit, or UAF) that reports to the National Anti-Money Laundering Committee, and has the mandate to receive financial disclosures and STRs from both financial and nonfinancial reporting entities, as well as present leads to the prosecutors' office. According to the GODR, the UAF, which became operational in 2005, has replaced the UIF as the FIU of the Dominican Republic. As a result, the UIF, which became a member of the Egmont Group in 2000, lost its membership in November 2006 as it is no longer the legally recognized FIU of the Dominican Republic. The UAF anticipates applying for Egmont membership once a full transition of FIU functions and responsibilities are complete, projected to occur by the end of the summer in 2009. Although the UAF is now recognized as the GODR's financial intelligence unit, it appears that there is still confusion among obligated entities regarding their reporting requirements. In 2007, rather than reporting directly to the UAF, reporting entities filed 824 STRs with the UIF. The UIF then reported the STRs to the UAF. The majority of the reports the UAF received in 2007 are thought to have been transferred from the UIF.

Further confounding the duality of FIU functions in the Dominican Republic is the proposed creation of an offshore financial center with its own agency equivalent to an FIU. In December 2008, legislation was passed by the Dominican Congress to allow for the creation of an Independent Financial Center of the Americas (IFCA), which would not be subject to the regulatory authority of GODR banking supervisors. Among the financial services proposed to be available will be businesses and investment banking, public and private brokerage, trading of titles and commercial paper, money and asset management. To reassure international concerns regarding the IFCA's susceptibility to abuse by money launderers and terrorist financiers, as well as the GODR's inability to ensure that the IFCA complies with anti-money laundering and counterterrorist financing standards, the creators of the IFCA have proposed establishing their own FIU to report to the UAF and exchange information with other FIUs. However, an FIU must by definition be a single, national entity. Although the creators proposed changing the name of the IFCA's FIU equivalent agency to avoid confusion, it would still serve as a filter for STRs that should be sent to the UAF, which is not permissible under the international standards of the Egmont Group and Financial Action Task Force.

In August 2008, the Government of the Dominican Republic (GODR) criminalized terrorist financing with the enactment of the Anti-Terrorism Law. The GODR continues to support U.S. Government efforts to identify and block terrorist-related funds. While no assets have been identified or frozen, the GODR 's efforts to identify and block terrorist-related funds continue through orders and circulars issued by the Ministry of Finance and the Superintendence of Banks that instruct all financial institutions to continually monitor accounts.

According to U.S. law enforcement officials, cooperation between law enforcement agencies on drug cases, human trafficking, and extradition matters remains strong. In 2008, GODR and U.S. law enforcement continued to work together to intercept and disrupt bulk cash smuggling organizations operating in the airports and seaports of the Dominican Republic. Law enforcement in the Dominican Republic continues targeting commercial flights and vessels that operate to drug source countries to disrupt the illicit money flow back to narcotics traffickers. In view of the recent increase in asset

forfeiture cooperation with the U.S., the Dominican Republic has requested that the U.S. enter into an Asset Sharing Agreement to better streamline future sharing efforts.

In July 2008, the National Drugs Control Agency (DNCD) raided exchange businesses used by a Dominican-Colombian drug ring that laundered millions of dollars through "Operation Pitufo" (Smurf). The DNCD and the U.S. Drug Enforcement Administration (DEA) exchanged information to identify others implicated in the money-laundering organization.

In June 2008, the Dominican Republic made a substantial asset seizure relating to a Medicare fraud prosecution in the Southern District of Florida involving a large amount of assets purchased by Luis, Carlos, and Jose Benitez (the Benitez Brothers) brothers. Of the $110 million dollars in fraudulent funds obtained, over $30 million were invested in assets in the Dominican Republic. Assets included a hotel, water park, houses, helicopter, seafront apartments, and automobiles. The Government of the Dominican Republic's (GODR) Prosecutor General's office assisted the Federal Bureau of Investigation agents in conducting the seizures. This is an on-going case at this time, and the United States anticipates taking over the forfeiture through litigation in Miami, Florida. The two countries are working closely together to discover additional assets in this, and other fraud cases, so that restitution may be made to victims of the fraud in the United States. The United States generally shares a large part of any confiscations that result from cooperation between the two countries on drug cases, and other nonvictim criminal matters, with the Dominican Republic.

In September of 2008, ICE conducted a month long enforcement operation with GODR Customs and National Police consisting of teams at various airports and at the ferry to Puerto Rico focusing on identifying individuals who failed to declare currency in excess of $10,000. The operation, conducted at airports around the country and the ferry terminal in Santo Domingo, resulted in 15 currency seizures totaling over $340,000. This was the most recent of several similar operations and ICE will continue to coordinate similar operations on a routine basis.

The Dominican Republic is a member of the Organization of American States (OAS) and the Caribbean Financial Action Task Force (CFATF)- a FATF-style regional body. The Dominican Republic and the United States do not have a mutual legal assistance treaty in place. The United States continues to encourage the GODR to sign and ratify the Inter-American Convention on Mutual Assistance in criminal matters, and to sign related money laundering conventions. The Dominican Republic is a party to the 1988 UN Drug Convention, the UN Convention against Corruption, the UN Convention against Transnational Organized Crime and, the UN Convention for the Suppression of the Financing of Terrorism.

The Government of the Dominican Republic (GODR) continues to enhance its anti-money laundering regime; however, additional improvements are still needed, particularly with regard to combating terrorist financing. While legislative and oversight provisions are being put in place in the formal financial sector, there still exists a lack of coordination among the various entities tasked with anti-money laundering activities. Weak implementation of anti-money laundering legislation leaves the Dominican Republic vulnerable to criminal financial activity. The Government of the Dominican Republic should enhance supervision of the nonfinancial sector, to ensure this sector's compliance with reporting requirements. The GODR should bolster the operational capacity of the fledgling UAF and ensure a full transition of FIU functions. With adequate personnel and enhanced capability, GODR officials working jointly with U.S. Law Enforcement agencies will have a greater capacity to conduct more effective money laundering investigations. The GODR should devote its resources to developing and implementing a viable anti-money laundering/counterterrorist financing regime that comports with international standards, and should not establish an offshore financial center, which would greatly increase the risk of all-source money laundering.

Ecuador

Ecuador is a major drug transit country, and as such, is vulnerable to money laundering. With a dollar economy geographically situated between two major drug producing countries, Ecuador is highly vulnerable to money laundering, although it is not an important regional financial center. Because only a few major banks have active money laundering controls in place, and because a large number of transactions take place through unregulated money exchange and remittance companies, there is no reliable way to judge the magnitude of such activity in the country. In addition to concerns about illicit transactions through financial institutions, there is evidence that money laundering is taking place through trade and commercial activity, as well as through trafficking of people. Weakly regulated casinos serve as an additional vulnerability for money laundering. Large amounts of unexplained currency entering and leaving Ecuador indicate that transit and laundering of illicit cash are also significant activities. Though smuggled goods are regularly brought into the country, there is no evidence that they are significantly funded by drug proceeds. Recent allegations, however, have surfaced about the possibility of Colombian drug traffickers' involvement in using Ecuador's financial system to launder drug proceeds through pyramid or Ponzi schemes.

Ecuador's financial sector consists of 29 banks, 13 investment companies, two formal exchange houses, 28 regulated cooperatives (and an estimated 600 to 800 additional unregulated, unlicensed and unsupervised cooperatives), 39 insurance companies, two stock exchanges, and eight mutual funds. Several Ecuadorian banks maintain offshore offices. The Superintendency of Banks and Insurance is responsible for oversight of both offshore and onshore financial institutions. Regulations are essentially the same for onshore and offshore banks, with the exception that offshore deposits no longer qualify for the government's deposit guarantee. Anonymous directors are not permitted. Licensing requirements are the same for offshore and onshore financial institutions. However, offshore banks are required to contract external auditors pre-qualified by the Superintendency of Banks. These private accounting firms perform the standard audits on offshore banks that would generally be undertaken by the Superintendency in Ecuador. Bearer shares are not permitted for banks or companies in Ecuador. Small local credit unions that provide loans and money transfers are numerous—approximately 5,800, according to tax authorities—and are regulated only by the Ministry of Social Affairs.

Law 2005-12 of October 2005 criminalizes money laundering in Ecuador. The law amends the Narcotics and Psychotropic Substance Act of 1990 (Law 108) and criminalizes the laundering of illicit funds from any source. It also penalizes the undeclared entry of more than $10,000 in cash or other convertible assets. The 2005 law also criminalizes money laundering in relation to any illegal activity, including drug trafficking, trafficking in persons, and prostitution. Money laundering is penalized by a prison term of one to nine years, depending upon the amount laundered, as well as a monetary fine. However, it is unclear if a conviction is required for the predicate offense to prosecute for money laundering.

Law 2005-12 establishes the National Council against Money Laundering, headed by the Procurador General (solicitor general) and includes representatives of all government entities involved in fighting money laundering, such as the Superintendency of Banks and the National Police. The law also establishes Ecuador's financial intelligence unit (FIU), the Unidad de Inteligencia Financiera (UIF), under the purview of the Council. There have been three UIF directors since the first was appointed in November 2006, with the most recent taking office in May 2008. The UIF became operational on December 1, 2007, and continues to strengthen its analytical capacity through technical assistance and improved software. An initiative under the new director has been to target casinos as potential sources of money laundering. During the year, the UIF promulgated two new regulations to strengthen monitoring and enforcement of the Money Laundering Law, one relates to casinos and the other to banks, cooperatives and credit unions. Under the new director, the UIF has referred 15 cases to the Attorney General's office for prosecution, with three of the cases related to casinos.

All entities that fall under the 1994 Financial System Law, including banks, savings and credit institutions, investment companies, stock exchanges, mutual funds, exchange houses, credit card administrators, money transmitters, mortgage companies, insurance companies and reinsurance companies, are required to report all "unusual and unjustified" transactions to the UIF within 48 hours. Financial institutions under the supervision of the Superintendency of Banks and Insurance currently report suspicious transactions to the Superintendency. Obligated entities are also required to establish "know-your-client" provisions, report cash transactions over $10,000 (including structured transactions amounting to more than $10,000 over a 30-day period), and maintain financial transaction records for ten years. Any person entering Ecuador with $10,000 or more in cash must file a report with the customs service; however, this requirement is currently not being enforced. Entities or persons who fail to file the required reports or declarations may be sanctioned by the Superintendency of Banks. The UIF may request information from any of the obligated entities to assist in its analysis of suspicious transactions, and cases that are deemed to warrant further investigation will be sent to the Ministry of the Public. The UIF is also empowered to exchange information with other financial intelligence units on the basis of reciprocity, and has entered into agreements with several countries to do so.

Some existing laws may conflict with the detection and prosecution of money laundering. For example, the Bank Secrecy Law severely limits the information that can be released by a financial institution directly to the police as part of any investigation, and the Banking Procedures Law reserves information on private bank accounts to the Superintendency of Banks. In addition, the Criminal Defamation Law includes sanctions for banks and other financial institutions that provide information about accounts to police or advise the police of suspicious transactions if no criminal activity is ultimately proven. The law also does not provide safe harbor provisions for bank compliance officers. The UIF is seeking legal reforms to address at least some of these issues.

Ecuador's first major money laundering case began in August 2006 with the arrest of approximately a dozen alleged members of a Colombian money laundering operation and the seizure of a large number of assets in Ecuador. The suspects were linked to accused drug trafficker Hernan Prada Cortes, who had acquired many Ecuadorian businesses and real properties in the names of other persons since 2000, and was extradited to the United States from Colombia. In February 2008, seven defendants in the case were convicted of money laundering, with prison sentences of four to eight years. The court also ordered the forfeiture of all seized assets to the state and the closing of six businesses. In August 2008, there was a second conviction under the 2005 Money Laundering Law, with an Ecuadorian female and Spanish male sentenced to three years and a fine of $265,000 for attempting to bring more than $500,000 into Ecuador illegally in July 2007.

In 2008, ICE and Ecuadorian customs authorities conducted joint interdiction operations in furtherance of ICE's Operation Firewall, a law enforcement effort focusing on the interdiction and investigation of bulk cash being smuggled around the world. The operations, conducted at airports in Quito and Guayaquil, resulted in the seizure of approximately $1,014,952. ICE is providing technical assistance to the Ecuadorian investigations.

Ecuador's legal system provides for asset forfeiture upon conviction; however, civil forfeiture is not permitted. The National Council against Money Laundering is responsible for administering the freezing and seizure of funds that are identified as originating from illicit sources. A special fund for forfeited assets will be set up in the Central Bank, and these assets will be distributed among government entities responsible for combating money laundering. No statistics are available on the amount of assets seized or frozen by the Government of Ecuador (GOE) in 2008.

Ecuador has not criminalized terrorist financing. The Ministry of Foreign Affairs, Superintendency of Banks and the Association of Private Banks formed a working group in December 2004 to draft a law against terrorist financing. In 2006, the draft law passed its first debate in Congress, but no further

actions were taken before the Congress went into recess and was replaced by a Constituent Assembly in 2007. In late 2008, the UIF developed a new draft law that included terrorist financing and was vetting it through government offices before introducing it to the legislature for approval. The Superintendency of Banks has cooperated with the U.S. Government in requesting financial institutions to report transactions involving known terrorists, as designated by the United States as Specially Designated Global Terrorists pursuant to Executive Order 13224, or as named on the consolidated list maintained by the United Nations 1267 Sanctions Committee. No terrorist finance assets have been identified to date in Ecuador. The Superintendency would have to obtain a court order to freeze or seize such assets, in the event they were identified in Ecuador. Currently, there are no measures in place to prevent the misuse of charitable or nonprofit entities to finance terrorist activities.

Following a referendum in September in which a new Constitution was approved, the government has been reorganizing the judiciary and considering various legal reforms. Among these possible reforms are changes to the Money Laundering Law, the Criminal Procedures Code and the Narcotics Law. The government is also considering adopting anti-terrorist financing and civil asset forfeiture legislation. While many of these proposed changes could greatly improve the prosecuting of money laundering and financial crime cases, it is too early to determine whether these changes will occur or what specifically they might entail.

Ecuador is a member of the Financial Action Task Force for South America (GAFISUD), and held the GAFISUD presidency in 2007. The GOE underwent a mutual evaluation by GAFISUD in September 2007, and the mutual evaluation report was accepted by the GAFISUD plenary in December 2007. The evaluation team found the GOE to be noncompliant or only partially compliant with 48 of the 49 Financial Action Task Force Recommendations on money laundering and terrorist financing. The mutual evaluation report noted the lack of a counterterrorist financing law and the lack of successfully prosecuted money laundering cases, but recognized that the UIF was making some progress.

Ecuador is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. The GOE is also a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Ecuador and the United States are parties to a bilateral Agreement for the Prevention and Control of Narcotics Related Money Laundering that entered into force in 1993, and a 1994 Agreement to Implement the United Nations 1988 Drug Convention as it relates to the transfer of confiscated property, securities and instrumentalities. There is also a Financial Information Exchange Agreement (FIEA) between the GOE and the United States to share information on currency transactions. The UIF has signed memoranda of understanding with the FIUs of Argentina, Brazil, Bolivia, Chile, Colombia, Panama, and Peru for the exchange of information.

The GOE has made progress in combating money laundering in recent years with the passage of anti-money laundering legislation and the establishment of an operational financial intelligence unit. However, the GOE should fully implement the existing legislation and ensure that reporting requirements are enforced. Ecuador is one of three countries in South America that is not a member of the Egmont Group of FIUs, and the GOE should ensure that the UIF becomes fully functional and meets the standards of the Egmont Group and the Financial Action Task Force. The GOE should criminalize the financing of terrorism to adhere to the UN Convention to which it is a party; such a step would also enable its FIU to apply for membership in the Egmont Group. The GOE should also address items that were not accounted for in its money laundering legislation, including the abolition of strict bank secrecy limitations and any potential sanctions for financial institutions that report suspicious transactions. Similarly, the GOE should amend its current legislation so that penalties applying to the laundering of funds under $5,000 are sufficiently dissuasive (the current penalty for laundering less than $5,000 is a fine of double the amount laundered and no prison terms apply), and

clarify whether a conviction for a predicate offense is required before prosecutors may charge an individual with money laundering. Finally, the GOE should take all necessary steps to comply fully with international anti-money laundering and counterterrorist financing standards to which it has formally committed through its membership in the UN, the OAS and GAFISUD.

Egypt, The Arab Republic of

Egypt is not considered a regional financial center or a major hub for money laundering. Egypt is becoming a more sophisticated financial center, but still has largely a cash economy. Many financial transactions do not enter the banking system. Egypt has a large informal economy as well, but data on the size of the informal economy is hard to come by. As part of its on-going economic reform plan, which began in 2004, the Government of Egypt (GOE) continued its financial sector reforms in 2008, and Egypt has received positive feedback from the World Bank and IMF on many of the financial sector reform efforts. However, some scheduled reform items were not completed in 2008, which may be partly attributable to global financial conditions. Accomplishments in 2008 included the launch of the small and medium size enterprise (SME) stock exchange, needed revisions to the capital markets law, and new amendments to the anti-money laundering law. One setback in 2008 was when efforts to privatize Banque du Caire (Cairo Bank) stalled after the Central Bank of Egypt (CBE) determined that none of the submitted bids met the government's minimum accepted bid. Few money laundering cases have made it to court in the last several years. While Egypt has improved supervision and the quality of its regulatory regime to prevent and fight money laundering, some activities continue which make Egypt vulnerable, including: illegal dealings in antiquities, corruption, misappropriation of public funds, smuggling, the use alternative remittance systems, and the misappropriation of public funds.

While there is no significant market for illicit or smuggled goods in Egypt, there is evidence that trade goods, arms, and cash are smuggled across Egypt's border with Gaza. The funding source is unclear, as is the destination of the proceeds. The under-invoicing of imports and exports by Egyptian businessmen is still a relatively common practice. The primary goal for businessmen who engage in such activity is reportedly to avoid taxes and customs fees, although those taxes and fees have been reduced in recent years. Customs fraud and invoice manipulation are also found in regional value transfer schemes and underground finance. A large portion of Egypt's economy remains undocumented and tax evasion remains a problem. The Ministry of Finance is attempting to address the evasion problem by improving the capacity of its anti-evasion unit and trying to obtain high profile prosecutions.

The CBE estimates that Egyptian expatriate workers remitted $8.5 billion in fiscal year 2007-2008. Western Union and Moneygram are the two primary formal cash transfer operators in Egypt. Egyptian authorities believe that informal remittance systems such as hawala are not a large phenomenon in Egypt, and therefore these systems are not monitored or regulated. As the black market for Egyptian pounds has dried up, the need for using alternative remittance systems has lessened. There are many overseas Egyptian workers, so as in many countries in the region, informal remittance systems exist. Those overseas workers who may be using informal means for convenience purposes, may do so because of lack of familiarity with banking procedures, desire to avoid fees, or because some banks require the sender to be an account holder.

Egypt's Law No. 80 of 2002 criminalizes laundering of funds from narcotics trafficking, prostitution and other immoral acts, terrorism, antiquities theft, arms dealing, organized crime, and numerous other activities. Law No. 80 provides the legal justification for providing account information to responsible civil and criminal authorities. The law established the Money Laundering Combating Unit (MLCU) as Egypt's financial intelligence unit (FIU), which officially began operating on March 1, 2003, as an independent entity within the CBE. The anti-money laundering law (AML) provides the main requirements of an anti-money laundering regime, such as record keeping, AML supervision,

reporting of suspicious transaction reports (STRs), protection from liability for reporting, and details of the penalties. The legal basis by which the MLCU derives its authority, also spells out the predicate crimes associated with money laundering, establishes a Council of Trustees to govern the MLCU, defines the role of supervisory authorities and financial institutions, allows for the exchange of information with foreign competent authorities, and set the detailed procedures for the implementation of Security Council Resolutions related to targeted financial sanctions. Article 86 of the Penal Code criminalizes the financing of terrorism.

In 2008, Law 80 was amended to strengthen the AML by including some additional categories of crimes that are now covered under the law. These include, insider trading, and customs evasion. The amendments also strengthened the role of MLCU within the GOE, requiring other competent government agencies to report to the MLCU any available information on money laundering crimes or the financing of terrorism. The amendment also requires that if a conviction judgment is passed in a money laundering case related to a legal person, that the judgment be published in two daily widespread newspapers and allows the judge to order suspension of the activities of the legal person for no more than one year.

After the promulgation of the new amendments, each one of the supervisory authorities (Central Bank of Egypt, Capital Markets Authority, Egyptian Insurance Supervisory Authority, General Authority for Investment and Free Zones, Ministry of Technology and Telecommunication and Mortgage Finance Authority) updated their own AML/CTF regulations and the FIU issued new know your customer (KYC) rules for each type of financial institutions.

The MLCU has its own budget and staff and full legal authority to examine all STRs and conduct investigations. Field investigations are administered by the FIU and conducted on behalf of the FIU with the assistance of law enforcement agencies, including the Ministry of Interior, the National Security Agency, and the Administrative Control Agency. Once concluded, results of investigations are sent back to the FIU for further examination and analysis. The FIU decides whether or not to forward the case to the public prosecutor. The MLCU shares information with appropriate agencies and those agencies are required to share information with the MLCU.

The MLCU is directed by a five-member Council of Trustees, which is chaired by the Assistant Minister of Justice for Legislative Affairs. Other members of the council include the Chairman of the Capital Markets Authority, the Deputy Governor of the CBE, a representative from the Egyptian Banking Federation, and an expert in financial and banking affairs. In June 2004, the MLCU was admitted to the Egmont Group.

Money laundering investigations are carried out by one of the three law enforcement agencies in Egypt, according to the type of predicate offense involved. The Ministry of Interior, which has general jurisdiction for the investigation of money laundering crimes, has a separate AML department that includes a contact person for the MLCU who coordinates with other departments within the ministry. The Ministry of Interior's AML department works closely with the MLCU during investigations. It has established its own database to record all the information received, including STRs, cases, and treaties. The Administrative Control Authority has specific responsibility for investigating cases involving the public sector or public funds. It also has a close working relationship with the MLCU. The third law enforcement entity, the National Security Agency, plays a more limited role in the investigation of money laundering cases, where the predicate offense threatens national security.

The CBE's Bank Supervision Unit shares responsibility with the MLCU for regulating banks and financial institutions and ensuring compliance with AML law. Under the AML law, banks are required to keep all records for five years, and numbered or anonymous financial accounts are prohibited. The CBE also requires banks to maintain internal systems enabling them to comply with the AML law and has issued an instruction to banks requiring them to examine unusual, including large, transactions. In addition, banks are required to submit quarterly reports showing compliance with respect to their

AML responsibilities. Improving the quality of the Supervision Department at the CBE has been a main tenant of the Bank reform effort. Reporting of suspicious transactions is compulsory by all banks and nonbank financial institutions.

Regulatory and supervisory authorities, including the CBE and MLCU undertake periodic on-site and off-site compliance assessments of all banks operating in Egypt. In the case of violations, banks are notified of corrective measures to be undertaken with a deadline for making the necessary changes. Compliance is ascertained via follow-up visits. Sanctions for noncompliance include issuing a warning letter, imposing financial penalties, forbidding banks to undertake certain activities, replacing the board of directors, and revoking the bank's license.

The CBE also monitors bureaux de change and money transmission companies for foreign exchange control purposes, giving special attention to accounts with transactions above certain limits. The CMA, which is responsible for regulating the securities markets, also conducts inspections of firms and independent brokers and dealers under its jurisdiction. Inspections are aimed at explaining and discussing AML regulations and obligations, as well as evaluating the implementation of systems and procedures, including checking for an internal procedures manual and ensuring the appointment of compliance officers.

The Egyptian Insurance Supervisory Authority (EISA) supervises insurance companies and controls for compliance with AML laws and regulations. The General Authority for Free Zones and Investment (GAFI) regulates activity in free zones and Special Economic Zones (SEZ). The Ministry of Communication and Information Technology regulates the Postal Authority and the financial services it offers. Egypt allows gambling in casinos located in international hotels, but only foreigners are allowed to enter the casinos. All cash transactions at casinos are performed by licensed banks subject to AML controls. Individuals acting as financial intermediaries, such as lawyers and accountants are not currently subject to AML controls. Prime Ministerial decree of 2008 added precious metal dealers and real estate brokers to the list of entities covered under the purview of the AML law.

Several recent laws and regulations govern the transportation of cash into the country. Law 88 of 2003 established the threshold for declaring foreign currency at borders to the equivalent of $10,000. The 2008 amendments added securities and commercial negotiable papers to the list of items that had to be declared if the value exceeds the equivalent of $10,000. The declaration requirement covers travelers leaving as well as entering the country. The 2008 amendments and accompanying executive regulations stipulate that the Customs Authority must enforce the law relating to cross-border movement of money. Enforcement of this provision is not consistent. The Customs Authority also signed an agreement with the MLCU to share information on currency declarations. Over the last few years there have been reports that Hammas officials repeatedly crossed the Egypt-Gaza border with millions of dollars in smuggled cash. Egyptian Customs Authorities at the Gaza Border must pass all reports of foreign currency declarations at the border to the MLCU, and also alert the European Union border guards of individuals crossing the border with large amounts of cash. Authorities state that terrorist attacks of the past several years have given extra impetus to law enforcement agencies to thoroughly scrutinize currency imports/exports.

Egypt is not an offshore financial center. Offshore banks, international business companies, and other forms of exempt or shell companies are not permitted in the country. Egypt has 9 public free zones, 250 private free zones, and one Special Economic Zone (SEZ). Public free zones are outside of Egypt's customs boundaries, so firms operating within them have significant freedom with regard to transactions and exchanges. The firms may be foreign or domestic, may operate in foreign currency, and are exempt from customs duties, taxes and fees. Private free zones are established by GAFI decree and are usually limited to a single project such as mixing, repackaging, assembling and/or manufacturing for re-export. The SEZs allow firms operating in them to import capital equipment, raw

materials, and intermediate goods duty-free and to operate tax-free. There is no indication that the zones are being used for trade-based money laundering schemes or for financing of terrorism.

The Law on Civil Associations and Establishments (Law No. 84 of 2002) governs the procedures for establishing nongovernmental organizations (NGOs), including their internal regulations, activities, and financial records. The law places restrictions on accepting foreign donations without prior permission from the proper authorities. The Ministry of Social Solidarity, with assistance from the Central Bank, monitors the operations of domestic NGOs and charities to prevent the funding of domestic and foreign terrorist groups.

Although the AML law does not specifically allow for seizure and confiscation of assets from money laundering, the Penal Code (Article 208aa) authorizes seizure and confiscation of assets related to predicate crimes, including terrorism. All assets are subject to seizure, including moveable and immoveable property, rights and businesses. Assets can only be seized with an order from the Public Prosecutor, and the agency responsible for seizing the assets depends on the predicate crime. Typically, the CBE seizes cash and the Ministry of Justice seizes real assets. Confiscated assets are turned over to the Ministry of Finance, and the executive regulations of the AML law allow for sharing of confiscated assets with other governments. The Public Prosecutor's office is currently engaged in negotiations to enhance cooperation with other governments on asset seizure and confiscation.

In January 2005, the National Committee for Combating Money Laundering and Terrorist Financing was established to formulate general strategy and coordinate policy implementation among the various responsible agencies of the GOE. The committee includes representatives from the Ministries of Interior, Foreign Affairs, Social Affairs, Justice, the National Security Agency, and the MCLU. The same agencies sit on a National Committee for International Cooperation in Combating Terrorism, which was established in 1998.

The GOE has made efforts to replace its emergency law, which has been in force since 1981, with anti-terror legislation. However, in 2008, the emergency law was extended again for another two years. It is unclear when the new anti-terror law will be brought before parliament and if it will include specific measures against terrorist financing.

The GOE and the United States have a Mutual Legal Assistance Treaty. Egyptian authorities have cooperated with U.S. efforts to seek and freeze terrorist assets. Egypt also has agreements for cooperation on AML issues with the United Kingdom, Romania, Zimbabwe, Peru, Canada, and Russia. The MLCU is responsible for circulating to all financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267, 1373, the United Nations Sanctions Committee's consolidated list, and the list of Specially Designated Global Terrorists designated by the U.S. pursuant to Executive Order 13224. The 2008 Prime Ministerial decree describes these responsibilities clearly. The MLCU is also charged with taking the legal measures to freeze the said actions. No known assets were identified, frozen, seized, or forfeited in 2008.

Egypt is a member of the Middle East and North Africa Financial Action Task Force (MENAFATF). Egypt was scheduled to undergo a Mutual Evaluation assessment with MENAFATF; however, it will be replaced by the World Bank's Financial Sector Assessment Programs (FSAP) that was conducted in late 2008. Egypt is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption and the UN International Convention for the Suppression of the Financing of Terrorism.

The quality of the Government of Egypt's anti-money laundering and terrorist finance regime will be based upon obtaining successful prosecutions and convictions. Egypt's regime continues to improve, but there are several areas that need improvement, particularly enhancement of investigative capacity dealing with financial crimes. Egypt should consider ways of improving the MLCU's feedback on

STRs to reporting institutions. It should improve its enforcement of cross-border currency controls, specifically allowing for seizure of suspicious cross-border currency transfers. Egyptian law enforcement and customs authorities should examine and investigate trade-based money laundering, informal value transfer systems, and customs fraud. The GOE should ensure that its updated law against terrorism specifically addresses the threat of terrorist financing, including asset identification, seizure and forfeiture.

El Salvador

The Government of El Salvador did not make any significant advances in 2008 to improve its ability to detect, investigate, and prosecute money laundering and financial crimes. The financial intelligence unit (FIU), the Unidad de Inteligencia Financiera, appears to be under used, and lacks institutional direction and investigative capacity. Only seven money laundering cases were brought to trial in 2008, and none resulted in any convictions. The government did request extradition from the United States of two high profile individuals in 2008.

Located on the Pacific coast of the Central American isthmus, El Salvador has one of the largest and most developed banking systems in Central America. The growth of El Salvador's financial sector, the increase in narcotics trafficking, the large volume of remittances through the formal financial sector and alternative remittance systems, and the use of the U.S. dollar as legal tender make El Salvador vulnerable to money laundering. Through August of 2008, approximately $2.6 billion in remittances were sent to El Salvador through the financial system. This is a decrease of approximately $900,000 from the previous year's total of $3.5 billion. The quality of additional remittances to El Salvador via other methods such as visiting relatives, regular mail and alternative remittance systems is not known. The Central America Four Agreement between El Salvador, Guatemala, Honduras, and Nicaragua allows for immigration inspection free movement of the citizens of these countries across their respective borders. As such, the agreement represents a vulnerability to each country for the cross-border movement of contraband and illicit proceeds of crime.

Most money laundering is conducted by international criminal organizations. These organizations use bank and wire transfers from the United States to disguise criminal revenues as legitimate remittances to El Salvador. The false remittances are collected and transferred to other financial institutions until sufficiently laundered for use by the source of the criminal enterprise, usually a narcotics trafficking organization.

Decree 498 of the 1998 "Law Against the Laundering of Money and Assets," criminalizes money laundering related to narcotics trafficking and other serious crimes, including trafficking in persons, kidnapping, extortion, illicit enrichment, embezzlement and contraband. The law also established the FIU within the Attorney General's office. The FIU has been operational since January 2000. The National Civilian Police (PNC) and the Central Bank also have their own anti-money laundering units.

Under Decree 498, financial institutions must identify their customers, maintain records for a minimum of five years, train personnel in identification of money and asset laundering, establish internal auditing procedures, and report all suspicious transactions and transactions that exceed approximately $57,000 to the FIU. Entities obligated to comply with these requirements include banks, finance companies, exchange houses, stock exchanges and exchange brokers, commodity exchanges, insurance companies, credit card companies, casinos, dealers in precious metals and stones, real estate agents, travel agencies, the postal service, construction companies, and the hotel industry. The law includes a safe harbor provision to protect all persons who report transactions and cooperate with law enforcement authorities, and also contains banker negligence provisions that make individual bankers responsible for money laundering at their institutions. Bank secrecy laws do not apply to money laundering investigations.

In 2008, the FIU identified 215 suspicious banking transactions, and categorized 667 cash transactions as possible instances of money laundering and/or financial crime. The FIU opened 19 formal investigations of suspected money laundering. The Attorney General's office brought seven money laundering cases to trial, but did not obtain any convictions. The FIU froze a total of $716,905 in funds suspected of being related to money laundering. In 2008, the Government of El Salvador (GOES) formally requested extradition of a former National Legislative Assembly Deputy facing public corruption and money laundering charges who had fled to the United States and was later apprehended in Anaheim, California and held on immigration charges. The GOES has also requested extradition of a fugitive financier apprehended in Miami, Florida who is wanted on charges of defrauding Salvadoran investors in a case dating back to 2005.

The GOES investigates private companies and financial service providers involved in suspicious financial activities. Despite demonstrating a greater commitment to pursue financial crimes, the GOES still lacks sufficient prosecutorial and police resources to adequately investigate and prosecute financial crimes. The GOES has established a secure computerized communication link between the Attorney General's office and the financial crimes division of the National Civilian Police. In addition to providing communication, the system has a software component that filters, sorts, and connects financial and other information vital to money laundering investigative capabilities. The FIU has reportedly attempted to establish a closer information sharing relationship with the Superintendent of the Salvadoran Financial System (SSF), as well as to formally incorporate the SSF into the existing secure computerized communication link.

To address the problem of international transportation of criminal proceeds, Decree 498 requires all incoming travelers to declare the value of goods, cash, or monetary instruments they are carrying in excess of approximately $11,400. Falsehood, omission, or inaccuracy on such a declaration is grounds for retention of the goods, cash, or monetary instruments, and the initiation of criminal proceedings. If following the end of a 30-day period the traveler has not proved the legal origin of said property, the Salvadoran authorities have the authority to confiscate the assets. In 2008, the GOES confiscated $859,621 in undeclared cash from travelers transiting Comalapa International Airport and other international land border crossings adjacent to Honduras and Guatemala. Of that total, $360,000 was seized as a result of joint interdiction operations at the airport by El Salvador Customs authorities and U.S. Immigration and Customs Enforcement (ICE) in furtherance of Operation Firewall, an ICE comprehensive law enforcement effort into the interdiction and investigation of global bulk cash smuggling.

The GOES has established systems for identifying, tracing, freezing, seizing, and forfeiting narcotics related and other assets of serious crimes. Forfeited money laundering proceeds are deposited in a special fund used to support law enforcement, drug treatment and prevention, and other related government programs, while funds forfeited as the result of other criminal activity are deposited into general government revenues. Law enforcement agencies are allowed to use certain seized assets while a final sentence is pending. In practice, however, forfeited funds are rarely channeled to counternarcotics operations. No legal mechanism exists to share seized assets with other countries. Salvadoran law currently provides only for the judicial forfeiture of assets upon conviction, and not for civil or administrative forfeiture. A draft law to reform Decree 498 to provide for civil forfeiture of assets, currently in the national legislature, has run into resistance from businessmen and others who are fearful that a civil asset forfeiture regime could lead to a crackdown on tax evaders, or possibly be misused for political purposes. In 2008, the GOES froze $716,905 in bank deposits related to money laundering and financial crime investigations.

The GOES passed counterterrorism legislation, Decree 108, in September 2006. Decree 108 further defines acts of terrorism and establishes tougher penalties for the execution of those acts. Article 29 of Decree 108 establishes the financing of terrorism as a criminal offense, punishable by a prison term of 20 to 30 years and a monetary fine ranging from $100,000 to $500,000. The law also granted the

GOES the legal authority to freeze and seize suspected assets associated with terrorists and terrorism. However, provisions to improve supervision of cash couriers, wire transfers, and financing of nongovernmental organizations (NGOs) were included in an early draft but not included in the final law.

The GOES has circulated the names of suspected terrorists and terrorist organizations listed on the United Nations (UN) 1267 Sanctions Committee consolidated list to financial institutions. These institutions are required to search for any assets related to the individuals and entities on the consolidated list. There is no evidence that any charitable or nonprofit entity in El Salvador has been used as a conduit for terrorist financing.

El Salvador has signed several agreements of cooperation and understanding with financial supervisors from other countries to facilitate the exchange of supervisory information, including permitting on-site examinations of banks and trust companies operating in El Salvador. El Salvador is also a party to the Treaty of Mutual Legal Assistance in Criminal Matters signed by the Republics of Costa Rica, Honduras, Guatemala, Nicaragua, and Panama. Salvadoran law does not require the FIU to sign agreements to share or provide information to other countries. The FIU is also legally authorized to access the databases of public or private entities. The GOES has cooperated with foreign governments in financial investigations related to narcotics, money laundering, terrorism, terrorist financing and other serious crimes.

El Salvador is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force (CFATF), a FATF-style regional body. The FIU has been a member of the Egmont Group since 2000. The GOES is party to the UN Convention for the Suppression of the Financing of Terrorism, the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption.

El Salvador should strengthen its ability to investigate and prosecute financial crime and improve its mechanisms for seizing and sharing assets. The GOES should ensure the passage of the civil asset forfeiture legislation that is currently under consideration by the legislature. Remittances remain an important sector of the Salvadoran economy and as such should be carefully supervised. The GOES should improve supervision of cash couriers and wire transfers and enact legislation requiring supervision of nongovernmental organizations to comport with international counterterrorism financing norms. The GOES should also ensure that sufficient resources are provided to the Attorney General's office as well as to the financial crime and narcotics divisions of the National Civilian Police.

France

France remains an attractive venue for money laundering because of its sizable economy, political stability, and sophisticated financial system. Narcotics-trafficking, human trafficking, smuggling, and other crimes associated with organized crime are among its vulnerabilities.

The Government of France (GOF) first criminalized money laundering related to narcotics-trafficking in 1987. Law 96-392 criminalizes the laundering of proceeds of all crimes. In 2004, the French Supreme Court ruled that joint prosecution of individuals was possible on both money laundering charges and the underlying predicate offense. Prior to this judgment, the money laundering charge and the predicate offense were considered the same offense and could only be prosecuted as one offense. French law has obliged institutions to combat money laundering since 1990. Entities obligated to file suspicious transaction reports (STRs) include those within a variety of financial and nonfinancial sectors, including banks, insurance companies, casinos, and lawyers.

Under Article 324 of the Penal Code, money laundering carries a penalty of five years imprisonment and a fine of 375,000 euros (approximately $525,000). With aggravating circumstances such as habitual or organized activity or connection with narcotics-trafficking (Article 222-38), the penalty increases to ten years imprisonment and a fine of 750,000 euros (approximately $1,050,000). The legal procedure for criminal conspiracy applies to money laundering crimes.

On August 4, 2008, the Parliament passed a law containing a provision allowing the government to transpose the European Union's (EU) Third Anti-Money Laundering Directive via government order (ordonnance). No such order had been published as of December 2008. In January 2009, the European Commission made the decision to refer France to the European Court of Justice over non-implementation of the Directive, which requires members to update their anti-money laundering (AML) regimes to comport with the most up-to-date standards, particularly with regard to regulation and terrorism financing.

France has developed the Liaison Committee against the Laundering of the Proceeds of Crime, which is comprised of representatives from reporting professions and institutions, regulators, and law enforcement authorities. The Committee's purpose is to share information with regulated entities and to make proposals to improve the AML system. The Justice Ministry and the French financial intelligence unit (FIU), known as the Unit for Treatment of Intelligence and Action Against Clandestine Financial Circuits (TRACFIN), co-chair this group.

The Banking Commission supervises fiduciary institutions and conducts regular audits of credit institutions. The Insurance and Provident Institutions Supervision Commission reviews insurance brokers. The Financial Market Authority monitors the reporting compliance of the stock exchange and other nonbank financial institutions. The Central Bank (Banque de France) oversees management of the records required to monitor banking transactions. Bank regulators and law enforcement can access the French Tax Administration's database to obtain information on the opening and closing of accounts. Information is available for depository accounts, transferable securities, and other properties, including cash assets. These records are important tools in the French arsenal for combating money laundering and terrorist financing.

TRACFIN is responsible for analyzing STRs filed by obliged entities. TRACFIN may exchange information with foreign counterparts that observe similar rules regarding reciprocity and confidentiality of information. TRACFIN works closely with the Ministry of Interior's Central Office for Major Financial Crimes (OCRGDF), which is the main point of contact for Interpol and Europol in France. TRACFIN can obtain information from senior police officers and central or local governments. The State Prosecutor informs the FIU of final court orders relating to suspicious transactions that have been reported.

TRACFIN received 12,481 STRs in 2007. The banking sector submits approximately 81 percent of STRs. The FIU referred 410 cases to the judicial authorities in 2007. In 2006, French courts convicted 126 individuals for money laundering, aggravated money laundering and laundering of narcotics-trafficking proceeds.

In addition to STRs, French law requires two other types of reports be submitted to the FIU. An entity must file a report with TRACFIN when the identity of the principal or beneficiary remains unclear despite due diligence. As with STRs, there is no threshold limit for such reporting. Entities must also file reports when a financial entity acting in an asset management capacity, or on behalf of another party acting in an asset management capacity carries out a transaction on a third party's behalf, when legal or beneficial owners are unknown. The reporting obligation can also be extended by decree to transactions carried out by financial entities, on their own behalf or on behalf of third parties, with natural or legal persons, including their subsidiaries or establishments, that are domiciled, registered, or established in any country or territory included on any list of noncooperative countries or territories developed by the Financial Action Task Force (FATF).

Law No. 96-392 of 1996 institutes procedures for seizure and confiscation of the proceeds of crime. French law permits seizure of all or part of property. In cases of terrorist financing, France has promulgated an additional penalty of confiscation of the total assets of the terrorist offender.

Since 1986, French counterterrorism legislation has provided for the prosecution of those involved in terrorist financing under the offense of complicity in the act of terrorism. To strengthen this provision, in 2001, France enacted a terrorist financing offense (Article 421-2-2 of the Penal Code) that follows the definition set forth in the UN Convention for the Suppression of the Financing of Terrorism and can result in ten years' imprisonment and a fine of 225,000 euros (approximately $303,750). In 2007, TRACFIN referred 17 cases of suspected terrorist financing to the judicial authorities for prosecution. TRACFIN participates in the "Cell for the Fight Against the Financing of Terrorism," an informal group created within the French Ministry of the Economy, Finance, and Industry to gather information to fight terrorist financing.

The GOF moved to strengthen France's anti-terrorism legal arsenal with the Act of 23 January 2006 (the Act), which entered into force by presidential decree in April 2007. This act empowers the Minister of the Economy to freeze the funds, financial instruments and economic resources belonging to individuals committing or attempting to commit acts of terrorism, and those belonging to companies directly or indirectly controlled by these individuals. Authorities can freeze accounts and financial assets through both administrative and judicial measures. By granting explicit national authority to freeze assets, the Act closes a potential loophole concerning the freezing of a citizen's assets as opposed to a resident EU-member citizen's assets. Under the new legislation, France also created a national terrorist list, which allows for the implementation of UNSCR 1373 concerning terrorism.

French authorities have moved rapidly to identify and freeze financial assets of organizations associated with al-Qaida and the Taliban under UNSCR 1267. The GOF takes actions against other terrorist groups through the EU-wide Working Party on implementation of Common Position 2001/931/CFSP on the application of specific measures to combat terrorism (931 Working Party), which replaces the previous informal EU "clearinghouse" procedure. Within the Group of Eight, France has sought to support and expand efforts targeting terrorist financing. France has worked to engage and improve the AML and counterterrorist financing (CTF) capabilities of some African countries by offering technical assistance. On the operational level, French law enforcement cooperation targeting terrorist financing continues to be strong.

The United States and France entered into a mutual legal assistance treaty (MLAT) in 2001. Through MLAT requests and by other means, the French have provided large amounts of data to the United States in connection with terrorist financing. TRACFIN is a member of the Egmont Group and Egmont Committee and has information-sharing agreements with 32 foreign FIUs. In 2007, TRACFIN filed 882 criminal intelligence requests and responded to 883 from counterparts under these agreements.

France is a member of the FATF. It is a Cooperating and Supporting Nation to the Caribbean Financial Action Task Force (CFATF) and an Observer to the Financial Action Task Force of South America (GAFISUD), both FATF-style regional bodies. France is a party to the 1988 UN Drug Convention; the UN Convention against Transnational Organized Crime; the UN Convention for the Suppression of the Financing of Terrorism; and the UN Convention against Corruption.

The Government of France has established a comprehensive AML regime and is an active partner in international efforts to control money laundering and the financing of terrorism. France should continue its active participation in international organizations and its outreach to lower-capacity recipient countries to combat the domestic and global threats of money laundering and terrorist financing. France should ensure the promulgating regulations for compliance with the Third Money Laundering Directive are fully effective, and the supervisory authorities are well-equipped to handle all of their pertinent duties. The GOF should enact a compulsory written cash declaration regime at its

airports and borders to ensure that travelers entering and exiting France provide, in writing, a record of their conveyance of currency or monetary instruments that can be saved and shared.

Germany

Germany is one of the largest financial centers in Europe. Most of the money laundering that occurs in Germany relates to white-collar crime. Although not a major drug producing country, Germany continues to be a consumer and a major transit hub for narcotics. Organized criminal groups involved in drug-trafficking and other illegal activities are an additional source of money laundering in Germany. Germany is not an offshore financial center.

In 2002, the Federal Republic of Germany (FRG) enacted a number of laws to improve law enforcement's ability to combat money laundering and terrorist financing. Among other provisions, the measures mandate suspicious activity reporting by a variety of entities, including notaries, accountants, tax consultants, casinos, luxury item retailers, and attorneys.

In May 2002, the German banking, securities, and insurance industry regulators merged into a single financial sector regulator known as the Federal Financial Supervisory Authority (BaFIN). Germany's anti-money laundering (AML) legislation requires that BaFIN maintain a centralized register of all bank accounts, with electronic access to all key account data held by banks in Germany. Banks cooperate with German authorities. Many have independently developed risk assessment software to screen potential and existing clients and their financial activity, and to monitor transactions for suspicious activity.

Germany's Money Laundering Act, amended by the Act on the Improvement of the Suppression of Money Laundering and Combating the Financing of Terrorism of August 8, 2002, criminalizes money laundering related to narcotics-trafficking, fraud, forgery, embezzlement, and membership in a terrorist organization. It also increases due diligence and reporting requirements for banks and financial institutions and requires financial institutions to obtain customer identification for transactions conducted in cash or precious metals exceeding 15,000 euros (approximately $20,250). The legislation mandates more comprehensive background checks for owners of financial institutions and tighter rules for credit card companies. Banks must report suspected money laundering to the financial intelligence unit (FIU) as well as to the State Attorney (Staatsanwaltschaft).

In August 2008, new legislation entered into force that contains further provisions on customer due diligence and other internal risk-management measures to prevent money laundering and terrorist financing. The new regulations apply to banks, insurance companies, and a number of professional groups (e.g., financial services providers, lawyers, notaries public, tax advisors, and other business operators). Suitable control structures ensure that proper, accurate and current information is available about the contracting party, to ensure transparency. The new law also expands reporting requirements to encompass transactions that support the financing of terrorism. A European Union (EU) regulation on wire transfers (EC 1781/2006) entered into force on January 1, 2007.

As an EU member, Germany complies with a recent EU regulation requiring accurate originator information on funds transfers for transfers into or out of the EU.

As of June 15, 2007, travelers entering Germany from a non-EU country or traveling to a non-EU country with 10,000 euros (approximately $13,500) or more in cash must declare their cash in writing. The definition of "cash" includes currency, checks, traveler's checks, money orders, bills of exchange, promissory notes, shares, debentures, and due interest warrants (coupons). The written declaration must also include personal data, travel itinerary and means of transport as well as the total amount of money being transported, its source, its intended purpose, and the identities of the owner and the payee. If authorities doubt the information given, or if there are other grounds to suspect money laundering or the funding of a terrorist organization, the cash will be placed under customs custody

until the matter has been investigated. Penalties for nondeclaration or false declaration include a fine of up to one million euros (approximately $1,345,000).

In May 2008, a 29-year old student attempted to depart Frankfurt International Airport with 8.7 million euros (approximately $11,750,000) in currency in his suitcases. The money, consisting of 50 and 100 euro notes, was confiscated and the State Prosecutor opened an investigation.

In September 2008, Germany participated in a multi-national customs cash smuggling operation that included most of the EU as well as a number of North African nations. Frankfurt-based representatives of the Department of Homeland Security Immigration and Customs Enforcement assisted in the coordination of the operation by providing real-time intelligence support to the German command center. During this week-long operation, 800 German customs agents stopped cars along the border in the direction of Switzerland and Liechtenstein. On roads, at airports, and on trains, a total of 13,000 persons and 22,000 pieces of luggage were inspected. In this operation, 181 cases of money smuggling were discovered and 5.5 million euros (approximately $7,425,000) was seized.

Germany has established a single, centralized, federal FIU within the Federal Office of Criminal Investigation (Bundeskriminalamt or BKA). Staffed with financial market supervision, customs, and legal experts, the FIU is responsible for analyzing cases, responding to reports of suspicious transactions, and developing and maintaining a central database of this information. Another unit under the BKA, the Federal Financial Crimes Investigation Task Force, combines 30 specialists in banking and financial transactions from the BKA and Federal Customs Authority to investigate money laundering cases.

Information for 2008 was unavailable, but in 2007, obligated entities filed 9,080 suspicious transaction reports (STRs) pursuant to the Money Laundering Act. According to the FIU's 2007 annual report, the 9,080 STRs generated 3,933 indications of potential criminal offenses. In comparison, the 10,051 STRs filed in 2006 generated 2,789 indications of criminal violations. The majority of the STRs with potential criminal indications, 3,248 of the 3,933 or 83 percent, cited fraud, including "phishing" and the use of "financial agents", as possible criminal offenses from the perspective of the reporting party. The individuals recruited in phishing schemes may be liable for money laundering penalties as well as for the illegal provision of financial services. Document forgery and tax offenses were the next most frequently cited offenses.

In 2007, approximately 59 percent of the persons cited in German STRs were German nationals. Of the 41 percent of the STRs that referenced non-German nationals, suspects with Turkish citizenship comprised the greatest proportion followed by Russian, Polish, Kazakh, Iranian, Italian, and Ukrainian nationals. The 2007 statistics on STRs concerning transfers of assets to and from foreign countries displayed a number of trends. As in 2006, Russia and the Ukraine remained the top two destinations for asset transfers that generated STRs in 2007. On STRs reporting transfers of assets from foreign countries to Germany, Russia is the most frequently cited source nation followed by the U.S., Kazakhstan, the United Kingdom, and Switzerland.

As with other crimes, actual enforcement of money laundering laws under the German federal system takes place at the state (sub-federal) level. Each state has a joint customs/police/financial investigations unit (GFG), which works closely with the federal FIU. The State Attorney can order a freeze of accounts when warranted.

Germany moved quickly after September 11, 2001, to identify and correct the weaknesses in its laws that had permitted terrorists to live and study in Germany. One reform package closes loopholes that had permitted members of foreign terrorist organizations to engage in fundraising in Germany (e.g., through charitable organizations). Subsequently, Germany increased its law enforcement efforts to prevent misuse of charitable entities. Germany has used its Vereingesetz, or Law on Associations, to

take administrative action to ban extremist associations that "threaten the democratic constitutional order."

A second reform package enhances the capabilities of federal law enforcement agencies and improves the ability of intelligence and law enforcement authorities to coordinate efforts and to share information on suspected terrorists. The law also provides Germany's internal intelligence service with access to information from banks and financial institutions, postal service providers, airlines, and telecommunication and Internet service providers. In 2002, the FRG also added terrorism and terrorist financing to its list of predicate offenses for money laundering, as defined by Section 261 of the Federal Criminal Code. The Criminal Code allows prosecution of members in terrorist organizations based outside Germany.

An amendment to the Banking Act institutes a broad legal basis for BaFIN to order frozen assets of EU residents suspected as terrorists. Authorities primarily concentrate on financial assets. BaFIN's system allows immediate identification of financial assets that can be potentially frozen, and German law enforcement authorities can freeze accounts for up to nine months. However, unless the assets belong to an individual or entity designated by the UNSCR 1267 Sanctions Committee, the FRG cannot seize money until authorities prove in court that the funds were derived from criminal activity or intended for terrorist activity.

Germany participates in United Nations and EU processes to monitor and freeze the assets of terrorists. The names of suspected terrorists and terrorist organizations listed on the UNSCR 1267 Sanctions Committee's consolidated list and those designated by EU or German authorities are regularly disseminated to financial institutions. A court can order the freezing of nonfinancial assets. Germany has taken the view that the EU Council Common Position requires, at a minimum, a criminal investigation to establish a sufficient legal basis for freezes under the EU 931 Working Party process. Proceeds from asset seizures and forfeitures go into the federal government treasury.

Since 1998, the FRG has licensed and supervised money transmitters, shut down thousands of unlicensed money remitters, and issued AML guidelines to the industry. German law considers the activities of alternative remittance systems such as hawala to be banking activities. Accordingly, German authorities require bank licenses for money transfer services, thus allowing authorities to prosecute unlicensed operations and maintain close surveillance over authorized transfer agents.

German law enforcement authorities cooperate closely at the EU level, such as through Europol. The German government has mutual legal assistance treaties (MLATs) with numerous countries. The FRG exchanges law enforcement information with the United States through bilateral law enforcement agreements and informal mechanisms, and the United States and German authorities have conducted joint investigations. The U.S. and FRG signed a MLAT in Criminal Matters on October 14, 2003. On July 27, 2006, the U.S. Senate ratified the MLAT and the German legislative bodies approved the implementing legislation in July and September 2007. Germany published the implementing legislation in the Federal Gazette on November 2, 2007, and the MLAT will come into effect once the parties formally exchange the instruments of ratification. Additionally, the U.S. and Germany signed bilateral instruments to implement the U.S.-EU Extradition and Mutual Legal Assistance Agreements on April 18, 2006. The approval process for these instruments, as well as the underlying U.S.-EU Agreements, continues and entry into force is expected in the near future. German authorities cooperate with U.S. authorities to trace and seize assets to the full extent allowed under German laws.

In March 2008, German authorities arrested a 24-year old Estonian at the request of the United States as he was transiting Frankfurt International Airport. The subject is charged with illegally accessing the computer systems of a national restaurant chain and stealing credit and debit card numbers from that system with total losses that could exceed $150,000,000. The subject was subsequently returned to the U.S.

German law currently does not permit the sharing of forfeited assets with other countries. Legislation implementing the EU Council Framework Decision 2006/783/JHA, on the application of the principle of mutual recognition of confiscation orders, is expected to enter into force by mid 2009. This legislation will allow for assets to be shared with other EU member states. The new legislation will also make it possible for Germany to share confiscated assets with non-EU member states on a case-by-case basis.

Germany is a member of the Financial Action Task Force, and the FIU is a member of the Egmont Group. Germany is party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. Germany has signed, but not yet ratified, the UN Convention against Corruption.

The Government of Germany's AML laws and its ratification of international instruments underline Germany's continued efforts to combat money laundering and terrorist financing. Germany should amend its wire transfer legislation to ensure that origination information applies to all cross-border transfers, including those within the EU. It should also amend legislation to waive the asset freezing restrictions in the EU 931 Working Party process for financial crime and terrorist financing, so that the freezing process does not require a criminal investigation; as well as amend its legislation to allow asset sharing with other countries. Germany should ratify the UN Convention against Corruption.

Ghana

Ghana is not a regional financial center, but as it develops, its financial sector is becoming more important regionally. Most of the money laundering in Ghana involves narcotics or public corruption. Ghana is a significant transshipment point for cocaine and heroin transiting from South America to Europe. Police suspect that criminals use nonbank financial institutions, such as foreign exchange bureaus, to launder the proceeds of narcotics trafficking. Criminals also launder illicit proceeds through investment in banking, insurance, real estate, automotive import, and general import businesses. Reportedly, donations to religious institutions have been used as a vehicle to launder money. The number of financial crimes, such as "advance fee" or 419 fraud letters (known as Sakawa in Ghana) and stolen credit and ATM cards originating in Ghana continues to increase.

Informal financial activity accounts for about 45 percent of the total Ghanaian economy. Ghana's 2000 census found that 80 percent of employment was in the informal sector. A small percentage of the informal economy uses the banking sector. Black market activity in smuggled goods is a concern because some traders smuggle goods to evade tax and import counterfeit goods. In most cases the smugglers bring the goods into the country in small quantities, and Ghanaian authorities have no indication that these smugglers have links to criminals who want to launder money gained through narcotics or corruption.

Ghana has designated four free trade zone areas, but the Tema Export Processing Zone is currently the only active free trade zone. Ghana also licenses factories outside the free zone area as free zone companies. Free zone companies must export at least 70 percent of their output. Most of these companies produce garments and processed foods. The Ghana Free Zone Board and the immigration and customs authorities monitor these companies. Immigration and customs officials do not think that trade-based money laundering (TBML) schemes are a major problem in the free trade zones. Although the Government of Ghana (GOG) has instituted identification requirements for companies, individuals, and their vehicles in the free zone, monitoring and due diligence procedures are lax.

The GOG has developed new laws to stimulate financial sector growth, including the revision of the banking law to strengthen the operational independence of the central bank, the Bank of Ghana. The government is promoting efforts to model Ghana's financial system on that of the regional financial hub of Mauritius. To this end, the GOG passed the Banking (Amendment) Act, 2007 Act 738, on June

18, 2007. The law establishes a provision for international banking services in Ghana and requires the Bank of Ghana to authorize offshore banks. Prior to this law, the Bank of Ghana licensed only reputable and internationally active banks. On September 7, 2007, Barclays Bank of Ghana Ltd., a subsidiary of Barclays Bank PLC, UK became the first bank to operate as an offshore bank. The Bank of Ghana is in the process of drafting regulations for offshore banks. A Financial Services bill, which will provide for Ghana's nonbank financial services, is before parliament and expected to be passed by the end of December 2008. To reduce duplication in processes and enhance information exchange, the law will establish a Financial Services Authority, which will absorb the functions of the National Insurance Commission and the Securities Exchange Commission. Ghana will then have two regulators for the financial services sector: the Bank of Ghana will be responsible for all banking and depository institutions, and the Financial Service Authority will handle all other financial services providers. The bill mandates that the two institutions establish a National Financial Services Coordination Committee to facilitate information exchange.

In January 2008 the Parliament passed Ghana's Anti-Money Laundering (AML) law. Accompanying regulations to the law have also been passed. The law identifies institutions subject to reporting and disclosure requirements; outlines the role of supervisory authorities; details preventive measures against money laundering; establishes customer identification and record keeping requirements; and institutes rules for required suspicious transaction reporting. Ghana's bank secrecy laws permit the sharing of information with relevant law enforcement agencies. Law enforcement officials can compel disclosure of bank records for drug-related offenses. Bank officials have protection from liability when they cooperate with law enforcement investigations.

The banking sector lacks a strong regulatory framework to prevent money laundering and ensure suspicious transaction reporting, although entities recognize the importance of such a framework. Local banks follow "know your customer" rules. The Bank of Ghana allows two types of foreign currency bank accounts: the foreign exchange (FE) account and the foreign currency (FC) account. The FE account is tailored to foreign currency sourced within Ghana while the FC account targets transfers from abroad. Bank of Ghana regulations instituted in December 2006 under the Foreign Exchange Act permit U.S. $10,000 per year to be transferred from an FE account without documentation and approval from the Bank of Ghana. The regulations also allow import transactions of up to $25,000 without initial documentation for FE accounts. There are no limits on the number of such transactions made on each account or on the number of such accounts that an individual can hold. The law does not permit foreign exchange bureaus to make outward transfers. Ghana has no effective system to obtain data on an individual's dealings with all the banks in Ghana.

The GOG established a National Coordinating Committee on July 16, 2008, comprised of approximately fifteen government departments and associations from obliged sectors. This body aims to implement a more efficient and cooperative response by the government and the private sector to prevent money laundering, terrorist financing, and other financial crimes in Ghana. The Committee has met several times since its inception.

Ghana has a cross-border currency reporting requirement. However, Ghanaian authorities have difficulty monitoring cross-border movement of currency. In a 2008 operation, the national security office detected that millions of dollars in repatriated foreign currencies has been entering Ghana through the Togo-Aflao border. An individual transports money from Ghana across the border undeclared and then returns through the same border, but declares the money on the Foreign Exchange Declaration Form. This maneuver allows the individual to take the money out of Ghana legally. In a bid to curb this, the Bank of Ghana issued a directive effective October 20, 2008, stating that the highest sum of money permitted to be carried by an individual arriving in the country is $10,000 or its equivalent. However, the Bank of Ghana's instructions include a number of options and circumstances that to conflict with the stated $10,000 limit, and has reportedly resulted in some confusion regarding the allowable amount for cross-border transportation vis-à-vis bank transfer.

The AML law calls for the establishment of a Financial Intelligence Unit (FIU), which will be called the Financial Intelligence Centre (FIC), and overseen by the National Security Council. The FIU will receive and analyze financial information, suspicious transaction reporting and intelligence, and disseminate an information package to law enforcement authorities for investigation. The FIU will have the authority to obtain information from other government regulatory authorities and from private sector financial institutions. The FIU has not yet been formed, although its site has been selected and offices are undergoing renovation. Ghana plans to fund the FIU through government grants and donations. The GOG is currently recruiting staff, some of whom will be current coordinating committee officers trained in money laundering and terrorist financing issues. In August 2008, the GOG arrested a flight attendant and two accomplices for attempting to launder £59,870 (approx. $90,121). The case is currently under prosecution. No arrests or prosecutions related to terrorist finance occurred in 2008.

The Narcotic Drug Law of 1990 provides for the forfeiture of assets upon conviction of a drug trafficking offense. A February 2007 court order compelled authorities to release seized assets from a 1991 landmark narcotics trafficking case, which resulted in a ten-year jail sentence of the convict, and return the assets to the owners. The ex-convict had appealed the seizure, arguing that the assets did not belong to him. The draft Proceeds of Crime bill, pending since 2006, contains provisions dealing with pre-emptive measures, confiscation and pecuniary penalty orders, search and seizure, and restraining orders and realization of property. Upon passage, the draft Proceeds of Crime bill will merge with the existing Serious Fraud Office Law, 1993 (Act 466). The Serious Fraud Office, established by this law, investigates corruption and crimes that have the potential to cause economic loss to the state.

In the past year, Ghana has criminalized the financing of terrorism, as required by United Nations Security Council Resolution 1373. On July 18, 2008, Parliament passed the Anti-Terrorism Bill, which came before Parliament in 2005. The law addresses terrorist acts, support for terrorist offenses, specific entities associated with acts of terrorism, and search, seizure, and forfeiture of property relating to acts of terrorism. The law imposes a term of imprisonment between seven and twenty-five years for any offense under the law. The Bank of Ghana has circulated the list of individuals and entities on the UNSCR 1267 Sanctions Committee's consolidated list to local banks, but no Ghanaian entities have identified assets belonging to any of the designees.

Although current Ghanaian law does not provide for the sharing of seized narcotics assets with other governments, the Narcotic Drug Law of 1990 includes provisions for the sharing of information, documents, and records with other governments. It also provides a basis for extradition between Ghana and foreign countries for drug-related offenses. The United States has not requested financial investigative assistance from Ghanaian authorities.

Ghana is a member of the Inter-Governmental Action Group Against Money Laundering and Terrorist Financing in West Africa (GIABA), a regional body modeled after the Financial Action Task Force (FATF). Ghana was scheduled to undergo its mutual evaluation in 2008, but after submitting its mutual evaluation questionnaire, requested that the date of the on-site assessment be moved from October 2008 to April 2009. Ghana has bilateral agreements for the exchange of money laundering-related information with the United Kingdom, Germany, Brazil, and Italy. Ghana is a party to the twelve UN conventions on terrorism, including the UN International Convention for the Suppression of the Financing of Terrorism. Ghana is a party to the 1988 UN Drug Convention, and the African Union Convention on Preventing and Combating Corruption. In June 2007, Ghana ratified the UN Convention against Corruption. Ghana has not signed the UN Convention against Transnational Organized Crime. Ghana has endorsed the Basel Committee's "Core Principles for Effective Banking Supervision."

The GOG should move swiftly to implement the AML Law, and should expand the list of predicate crimes to comply with international standards. The GOG should improve capacity among the agencies

impacted, and establish its FIU. The GOG should make every effort to pass asset seizure and forfeiture legislation that comports with international standards as soon as possible. Once the laws are in place, Ghana should take the necessary steps to promote public awareness and understanding of financial crime, money laundering and terrorist financing activities. Ghana should immediately release regulations and guidance for its new offshore entities, and draft legislation to ensure that offshore entities are treated identically to the onshore sector under the AML law. Additionally, the GOG should institute a beneficial ownership identification requirement and require that the true names of all onshore and offshore entities and their beneficial owners be held in a registry accessible to law enforcement. The GOG should increase cooperation and information sharing with other governments. Ghana should also become a party to the UN Convention against Transnational Organized Crime.

Gibraltar

Gibraltar is an overseas territory of the United Kingdom (UK). A November 2006 referendum resulted in constitutional reforms transferring powers exercised by the UK government to Gibraltar. Gibraltar is a significant international financial center with strong ties to London, the Channel Islands, Israel, Cyprus, and other financial centers. Located at the southern tip of Spain, near the north coast of Africa, Gibraltar is adjacent to known drug-trafficking and human smuggling routes. It is also a retail banking centre for northern Europeans with property in southern Spain. All of these factors contribute to money laundering and terrorist financing vulnerabilities in Gibraltar.

Gibraltar was one of the first jurisdictions to introduce and implement money laundering legislation that covers all crimes. The Gibraltar Criminal Justice Ordinance to Combat Money Laundering, which relates to all crimes, entered into effect in 1996. The Drug Offenses Ordinance (DOO) of 1995 and Criminal Justice Ordinance of 1995, amended in June 2007 as the Criminal Justice Act, criminalize money laundering related to all crimes. Gibraltar extended the Criminal Justice Act to include nonfinancial sectors. The laws mandate reporting of suspicious transactions by any obligated entity or individual. The DOO covers banks, mutual savings companies, insurance companies, financial consultants, postal services, exchange bureaus, attorneys, accountants, financial regulatory agencies, unions, casinos, charities, lotteries, car dealerships, yacht brokers, company formation agents, dealers in gold bullion, and political parties.

Criminal conduct is defined as any activity, either committed in Gibraltar or elsewhere, which if it had been conducted in Gibraltar would be indictable. This includes tax evasion, as the committal of such an offence would normally also include the committal of other indictable offences. The laws cover money laundering offenses related to acquisition, possession or use of property representing proceeds of criminal conduct, concealing or transferring proceeds of criminal conduct, tipping-off, and assisting others to retain the benefit of criminal conduct.

Authorities issued comprehensive anti-money laundering Guidance Notes, which have the force of law, to clarify the obligations of Gibraltar's financial service providers. Gibraltar issued its most recent Guidance Notes in December 2007 with amendments based on the Criminal Justice (Amendment) Act 2007 and Terrorist (Amendment) Act 2007. The 2007 Guidance Notes apply to banks and building societies, the Gibraltar Saving Bank, investment business, controlled activities, life insurance companies, currency exchangers/bureaux de change, and money transmission/remittance offices.

The Government of Gibraltar (GOG) permits Internet gaming that is subject to a licensing regime. Gibraltar has guidelines for correspondent banking, politically exposed persons (PEPs), bearer securities, and "know your customer" (KYC) procedures.

Gibraltar established the Financial Services Commission (FSC), a unified regulatory and supervisory authority for financial services, under the FSC Ordinance (FSCO) 1989. Required by statute to match the supervisory standards of the UK, the FSC is the supervisory body for banks and building societies;

investment businesses; insurance companies; and controlled activities, which include investment services, company management, professional trusteeship, insurance management and insurance intermediation. The main legal instruments governing the regulation and supervision of the financial system, in addition to the FSCO, are: the Banking Ordinance (1992) that provides powers to license and supervise banking and other deposit-taking business in Gibraltar; the Insurance Ordinance (1987) that provides powers to regulate and restrict the conduct of insurance business; and the Financial Services (Collective Investment Schemes) Ordinance that provide for the licensing and supervision of investment business.

Legislation requires all businesses to establish the beneficial owner of any company or asset before undertaking a relationship or incorporating any company or asset. Onshore and offshore banks are subject to the same legal and supervisory requirements. Institutions must retain financial records for at least five years from the date of completion of the business. If the obligated institution has submitted a suspicious transaction report (STR) to the Gibraltar financial intelligence unit (FIU) or when it knows that a client or transaction is under investigation, it is required to maintain any relevant record even if the five year interval has expired. If a law enforcement agency investigating a money laundering case cannot link the funds passing through the financial system with the original criminal money, then the funds cannot be confiscated.

The Financial Services Commission Act 2007 (FSCA), which became effective in May 2007, repeals and replaces the Financial Services Commission Act of 1989. This legislation modernizes and restructures the FSC. One of the most significant changes arising from the FSCA is in respect to the appointment of members of the Commission, who are selected by the minister with responsibility for financial services (presently the Chief Minister) from a short list of three suitable persons provided to him by existing members. The FSC also received expanded statutory functions. The FSC holds formal licensing, supervisory, and regulatory powers over all firms authorized under the Supervisory Acts. The FSC authority also ensures compliance with legislation, rules and guidance notes in general as well as those specific to combating financial crime. The FSC is able to issue Rules and Guidance, which enables the FSC to draft practical guidance for compliance with legislative measures, and regulatory expectations to supplement legislative provisions. As a safeguard against inappropriate or overregulation, the rules and guidance undergo a public consultation process and are subject to final veto of the Minister.

In 1996, Gibraltar established the Gibraltar Coordinating Center for Criminal Intelligence and Drugs (GCID) to receive, analyze, and disseminate financial information and reports filed by obligated institutions. The GCID serves as Gibraltar's FIU (GFIU) and is a sub-unit of the Gibraltar Criminal Intelligence Department. The GCID consists mainly of police and customs officers but is independent of law enforcement. The GFIU receives approximately 100 STRs per year.

Gibraltar's 2001 Terrorism (United Nations Measures) (Overseas Territories) Order criminalizes terrorist financing. The Order requires banks to report any knowledge that a present, past or potential client or customer is a terrorist, or receives funds in relation to terrorism, or makes funds available for terrorism. Gibraltar also addresses terrorist financing through the Terrorism Ordinance (2005). Among the terrorism-related offenses are: raising funds for terrorism, the use and possession of money or other property for terrorism, arranging funds for terrorism, and arrangement for the retention or control of terrorist property.

Application of the 1988 U.S.-UK Agreement Concerning the Investigation of Drug Trafficking Offenses and the Seizure and Forfeiture of Proceeds and Instrumentalities of Drug Trafficking was extended to Gibraltar in 1992. The DOO of 1995 provides for mutual legal assistance with foreign jurisdictions on matters related to narcotics trafficking and related proceeds. Gibraltar has passed legislation to update mutual legal assistance arrangements with its European Union and Council of Europe partners. Gibraltar is a member of the Offshore Group of Banking Supervisors (OGBS) and the

International Organization of Securities Commissions (IOSC). The GFIU is a member of the Egmont Group. Gibraltar has brought its laws into conformity with the obligations of states parties to the 1988 UN Drug Convention. On November 27, 2007, the UK Government extended to the Bailiwick the UN Convention against Transnational Organized Crime.

The Government of Gibraltar should continue its efforts to implement a comprehensive anti-money laundering/counterterrorist financing (AML/CTF) regime. The criminal laws on money laundering should be consolidated, and powers presently available only in drug-related money laundering cases should be extended to money laundering cases involving the proceeds of other crimes. The GOG should introduce legislative provisions to its asset seizure and confiscation regime allowing authorities to confiscate assets, including cash, even without a link to the original criminal proceeds. Gibraltar needs to conduct risk assessments of those designated nonfinancial businesses and professions that are unsupervised, and determine and extend the necessary authority to conduct AML/CTF compliance examinations of these entities.

Greece

Greece is becoming a regional financial center in the rapidly developing Balkans as well as a bridge between Europe and the Middle East. Anecdotal evidence of illicit transactions suggests an increase in financial crimes in the past three years. Greek law enforcement proceedings indicate that Greece is vulnerable to narcotics trafficking, trafficking in persons and illegal immigration, prostitution, cigarette and other forms of smuggling, serious fraud or theft, illicit gambling activities, and large scale tax evasion. While the government has made the pursuit of tax evasion a centerpiece of its economic reform agenda, there are few indications these reforms are having an impact. U.S. law enforcement agencies believe that criminally derived proceeds are not typically laundered through the Greek banking system. Instead, they are most commonly invested in real estate, the lottery, and the stock market. U.S. law enforcement agencies also believe Greece's geographic location has led to a moderate increase in cross-border movements of illicit currency and monetary instruments due to the increasing interconnection of financial services companies operating in southeastern Europe and the Balkans. Criminal organizations from southeastern Europe and the Balkan region execute a large percentage of crime generating illicit funds. The widespread use of cash facilitates a gray economy as well as tax evasion. Due to the gray economy, it is difficult to determine the amount of smuggled goods in the country. Currency transactions involving international narcotics-trafficking proceeds do not appear to include significant amounts of U.S. currency.

Greece has three free trade zones, located at the ports of Piraeus, Thessalonica, and Heraklion, where foreign goods may be imported without payment of customs duties or other taxes if they are subsequently transshipped or re-exported. There is no information regarding whether criminals use these zones in trade-based money laundering (TBML) or in terrorist financing schemes.

Greek authorities maintain that Greece is not an offshore financial center. Law 3427/2005, which makes reference to domestic and foreign companies, officially replaced Greek law 89/1967, which provided for the establishment of offshore entities. Under Law 3427, foreign and domestic companies may provide specific services to enterprises not established in Greece. These companies must employ at least 4 employees and have at least 100,000 euros ($130,594) in annual operating expenses in Greece. These entities must apply for a special license with the Ministry of Economy and Finance (MoEF) and, once the license is granted, file an application with the Directorate of Foreign Investments in the MoEF, the regulatory authority for companies covered under Law 3427/2005. The do not receive a tax exemption and must comply with anti-money laundering and counterterrorist financing (AML/CTF) law. Pursuant to Article 10 of Law 3691/2008, the MoEF will need to obtain and catalog additional registry information in order to comply with AML/CTF law.

Shipping companies, known for their complex corporate and ownership structures, and which reportedly can be used to hide the identity of the beneficial owner, are not governed by Law 3427, but rather by Laws 27/1975 and 378/1968. Although companies must keep a receipts and expenses book, they have no obligation to publish financial statements. These firms frequently fall under the authority of non-Greek jurisdictions and often operate through a large number of intermediaries, potentially serving as a vehicle for money laundering. Greek law allows banking authorities to check these companies' transactions, but authorities need the cooperation of other jurisdictions for audits to be effective.

Greek law does not provide for nominee directors or trustees in Greek companies. Previous laws had abolished bearer shares for banks and a limited number of other types of companies. The AML/CTF regime prohibits credit and financial institutions from allowing secret, anonymous, or number-identified accounts, anonymous passbooks, accounts in fictitious names, or accounts without the full names and identifying information of holders. The Government of Greece (GOG) maintains that various transparency laws mandate registered shares. The information available in the "Companies Registries" maintained by several authorities relates solely to the Board of Directors at the time of the incorporation of the company and does not log changes of directors, or the true beneficial owners of the company. Regional registries keep this information in a paper format. Greek law does not prohibit financial institutions from engaging in business with foreign financial institutions that allow their accounts to be used by shell companies.

The BOG maintains that alternative or informal remittance systems are illegal and do not exist in Greece, and it has no plans to introduce initiatives for their regulation. Nonprofit organizations fall within the purview of the Special Control Service (the tax police or YPEE) and the Ministry of Foreign Affairs. However, the GOG has not viewed charitable organizations as vulnerable to terrorist financing or money laundering and has not actively monitored such entities for these crimes. Each nonprofit organization must have a tax identification number, so their tax information is accessible by the financial intelligence unit (FIU). Despite these measures, these entities do not fall under AML/CTF regulation and are not supervised for AML/CTF compliance. The Ministry of Foreign Affairs plans to review the sector, and by the end of 2009, consider legislation to achieve transparency in the activities of nonprofits.

The June 2007 Financial Action Task Force (FATF) mutual evaluation report (MER) of Greece indicated that legal requirements in place to combat money laundering and terrorist financing did not meet international standards. The report articulated concerns about the overall effectiveness of the AML/CTF system, including inadequate customer identification programs and legal systems to prevent money laundering and terrorist financing, and a lack of adequate preventive measures and regulatory oversight.

Greece has had laws criminalizing terrorism, organized crime, money laundering and corruption since July 2002; however, the various laws did not include all categories of offenses, and the laws were poorly drafted, making enforcement difficult. After the adoption of the 2007 MER, the GOG passed new laws and implemented measures to enhance the effectiveness of its AML/CTF system. On August 5, 2008, Greece passed Law 3691/2008 that clearly defines money laundering and includes all offenses punishable by a minimum penalty of more than six months imprisonment. The law makes a money laundering conviction possible without a conviction for a predicate offense and extends the definition of illicit proceeds to include any type or value of property involved. It also removes tax confidentiality restrictions for purposes of AML/CTF reporting. Conviction for a money laundering offense carries a punishment of up to 10 years imprisonment and a fine of up to 1 million euros ($1.31 million). Law 3691/2008 mandates a risk-based approach for all financial institutions, now inclusive of bureaux de change and money remitters, with enhanced due diligence for some clients and politically exposed persons. The law also mandates identification of beneficial owners, defined as

individuals who own or control 25 percent plus one share of a legal entity. Under Act 25779/2006, the Bank of Greece (BOG) has applied these provisions to all financial institutions under its supervision.

Greece has three key authorities that supervise and monitor the financial sector: the Banking Supervision Department of the BOG, and the Hellenic Capital Market Commission (HCMC), and Private Insurance Supervision Commission (PISC), (both of which fall under the MoEF). All three entities have extensive supervisory programs and internal departments focused on AML/CTF and staffed with auditors, examiners, financial analysts, and lawyers. These authorities issue regulations, guidelines and circulars, and conduct on-site and off-site audits for AML compliance, special audits as needed, and outreach and training for compliance officers and stakeholders. The GOG gives the three supervisory entities resources and authorities to monitor, supervise and enforce the regulations.

The BOG, Greece's central bank supervises banks, bureaux de change, and money transmitters. The BOG conducts on-site examinations at least once every two years and off-site or special examinations as needed of entities under its supervision, including Greek banks located in other countries, The BOG hired additional examiners in 2008, and BOG staff attended specialized AML/CTF seminars.

The HCMC monitors compliance with the provisions of the capital market law, and as such supervises brokerage firms, investment firms, mutual fund management companies, portfolio investment companies, real estate investment trusts, financial intermediation firms, clearing houses and their administrators (e.g., the Athens stock market), and investor indemnity and transaction security schemes (e.g., the Common Guarantee Fund and the Supplementary Fund). The HCMC's AML/CTF unit includes three auditors who have received specialized AML/CTF training. HCMC can draw upon additional expertise as needed from the MoEF.

The PISC, created in January 2008, regulates and supervises the private insurance sector. Its AML/CTF supervision consists of two financial analysts and one lawyer, and can tap other PISC staff. The PISC has requested that each of its obliged entities submit their AML/CTF compliance procedures. PISC began evaluating these and conducting compliance audits at the end of 2008.

According to Article 6 of the new AML/CTF law, all designated nonfinancial businesses and professions (DNFBPs) and all trust and company service providers are subject to the AML/CTF law and have a competent authority. These competent authorities, together with the FIU, are responsible for providing AML/CTF guidance and feedback to entities under their competency in order to ensure that these entities are aware of and comply with their obligations under Law 3691/2008. The General Directorate of Tax Audits of the MoEF has, under the law, established a new unit to regulate and supervise entities under its control, including dealers in high value goods, pawnbrokers, and venture capital firms. The Gambling Control Commission established by Law 3229/2004 oversees casinos and other entities engaged in gambling or betting, including casinos operating on ships flying the Greek flag. Authorities have targeted the gaming industry to restrain money launderers from using Greece's nine casinos to launder illicit funds; however, up until now, there has been little regulatory oversight of the gaming industry.

Supervised institutions must send to their competent authority a description of the internal control and communications procedures they have implemented to prevent money laundering and terrorist financing. Banks must also undergo internal audits. Bureaux de change must send the BOG a monthly report on their daily purchases and sales of foreign currency. According to the FATF follow-up report, the reorganization of the BOG's AML/CTF supervision department should have a significant impact on the quality of targeted supervision carried out in bureaux de change and money remittance companies, and the new AML/CTF law and previous legislation is now applicable to these entities.

Under Law 3148, the BOG has direct scrutiny and control over transactions by credit institutions and entities involved in providing services for funds transfers, including electronic transfers. The BOG

issues operating licenses after assessing the institutions, their management, and their capacity to ensure the transparency of transactions.

Under Decree 2181/93, banks in Greece must demand customer identification information when a customer opens an account or conducts transactions exceeding 15,000 euros ($19,591). Banks must obtain specific documents from both natural and legal persons. Article 13 of Law 3691 includes requirements on collecting beneficial ownership information and measures relating to CDD requirements. Credit institutions must obtain identification documents when changing money, for all transactions exceeding 500 euros ($653). The law requires that banks and financial institutions maintain adequate records and supporting documents for at least five years after ending a relationship with a customer, or, in the case of occasional transactions, for five years after the date of the transaction. Banks suspecting illegal activity may take measures to gather more information on the identification of the person involved in the transaction, but, reportedly, in the past they have not done so.

Greek law requires every financial institution to appoint a compliance officer to whom all other branches or officers must report suspicious transactions. Both banks and nonbank financial institutions must submit suspicious transaction reports (STRs), though in practice, reportedly, the latter rarely do so. Obligations to report and to furnish all relevant information to prosecutorial authorities also apply to government employees involved in auditing, including employees of the BOG, the MoEF, the HCMC, and the PISC. In 2007, the FIU formalized the standard information required on STRs. Safe harbor provisions protect individuals reporting violations of AML laws and statutes.

Greece has adopted banker negligence laws under which individual bankers face liability if their institutions do not comply with AML/CTF laws and provisions, or do not file STRs. The new AML/CTF law provides the BOG with the authority to levy financial penalties that authorities believe are effective, proportionate and dissuasive. Financial sanctions include fines of up to 3 million or 500,000 euros ($3.92 million or $653,193) per legal entity or individual, respectively. The BOG planned to issue a directive to clarify and enhance transparency in the sanctions regime. The BOG may ask for the removal of the Internal Audit, Compliance or Risk Management Unit chiefs as well as any member of a Board of Directors if any has failed to achieve effective compliance. In the first five months of 2008, the BOG fined banks under its supervision a total of 805,000 euros ($3.1 million) for AML/CTF compliance violations. While the HCMC does not have data on fines levied in 2008, the amount in 2007 totaled 3.8 million euros ($4.97 million). As a new supervisor, the PISC has not yet implemented a fine structure; however, under the new law, it has the authority to do so.

Article 7 of Law 3691/2008 restructured the Greek FIU in order to try to address shortcomings described in the MER and increase the FIU's effectiveness. The revamped FIU, renamed the Commission for Combating Money Laundering and Terrorist Finance, began operations in September 2008. Although operationally independent, the FIU falls administratively within the Ministry of Finance and Economy. The Supreme Judicial Court appoints the FIU President, who presides over an FIU Board chosen from different ministries by the Ministers of Justice and Economy and Finance, and his alternate. The private sector no longer has a participatory role. This 8-member, part-time, Board coordinates with the competent authorities and the MoEF as Central Coordination Authority. The new law guarantees the FIU financial resources to fulfill its functions via an annex to the state budget. This also provides the FIU independence not granted previously.

To address staffing shortages, the new head of the FIU is hiring new staff. At the end of 2008, the FIU has 26 staff, comprised of police, financial analysts and IT experts seconded from other ministries. When fully staffed, the FIU will have 35 employees. The President of the FIU can also draw upon or other agencies as needed. The FATF follow-up opined that the number of substantive staff still appears insufficient to carry out the wide range of FIU functions.

The Greek FIU receives and processes all STRs. For each STR received, the FIU can access public and private files and demand information from financial, administrative, and law enforcement networks, notably YPEE and the police. The new AML/CTF law amends the bank secrecy law to allow the Greek FIU to receive classified, confidential, and secret information from banks. Although the FIU recently established a database to track STR submissions, it is reportedly insufficient to meet the FIU's needs, as the FIU still lacks modern technological elements. For example, STRs are hand delivered to the FIU on paper. The FIU's new leadership has designated a sophisticated STR database as an urgent priority, the MoEF has given assurance that funding is forthcoming, and a new database could be functioning by the end of 2009.

Greek authorities indicate that in 2008 the number of STRs increased and that the FIU expected to receive more than 2,600 reports total for the year. According to the follow-up report, due to longstanding problems, only about 1,100 STRs have been input into the FIU's system, resulting in a backlog of about 1,400. According to the FIU, as each new STR comes in, it will be analyzed in a timely manner. If the FIU considers an STR to warrant further investigation, it forwards the case to YPEE. When it decides there is enough information to commence prosecution, it forwards the case to the Public Prosecutor. Although the FIU has the authority to impose heavy penalties on those who fail to report suspicious transactions, it has not done so in the past.

YPEE falls under the direct supervision of the MoEF and has formal investigative authority over cases that, broadly defined, involve smuggling and high-value tax evasion. The FIU is responsible for preparing money laundering cases on behalf of the Public Prosecutor's Office, and works with YPEE to investigate cases that warrant further action. YPEE has its own in-house prosecutor to facilitate confidentiality and speed of action.

In the past, Greek authorities have not frequently prosecuted money laundering cases independent of the predicate offense, and according to the MER, limited data indicates a low rate of convictions on money laundering prosecutions. According to the GOG, since July 2007, a special team of prosecutors has focused on money laundering and terrorist financing issues, handling the majority of cases. The government has also increased financial crimes training for these prosecutors and judges. Despite these measures, there are still shortcomings. The Greek judicial system has one court handling all judicial activity related to money laundering and terrorist financing. Prosecutorial authorities lack an effective system to track money laundering prosecution statistics. The Ministry of Justice has yet to compile statistics related to arrests or prosecutions for money laundering or terrorist financing offenses, despite requests by the FIU and Greek Bar Association to do so. Under the new AML/CTF law, the services of the Ministry of Justice must ensure the collection, registry, and processing of financial crime data. The government has indicated it intends to develop systems to keep statistics.

Law 3691/2008 provides for confiscation of direct and indirect proceeds of a crime, and empowers the FIU to freeze direct and indirect assets of persons involved in money laundering cases. In addition, Greek authorities can now freeze assets in urgent money laundering and terrorist financing cases without first having to open a criminal investigation.

In addition, the new law establishes sanctions of up to 3 million euros ($3.99 million) for failing to freeze assets and funds. The GOG has indicated that the FIU will develop guidance for the financial and DNFBP sectors in the immediate future. Under the new law, an investigating judge or the judicial council can freeze assets temporarily with the consent of the Public Prosecutor. In addition, the FIU President or a Board member can temporarily freeze assets and notify the Public Prosecutor afterwards in order to conduct a further investigation. The new law provides for the seizure of assets upon conviction for an money laundering offense, fines of up to 2 million euros ($2.66 million) and a jail term of up to twenty years.

The YPEE has established a mechanism for identifying, tracing, freezing, seizing, and forfeiting assets of narcotics-related crimes, the proceeds of which are turned over to the government. YPEE

investigators have authorization to immediately seize property pending court review and seize property purchased with proceeds of narcotics trafficking or used to facilitate narcotics trafficking. Official forfeiture requires a court order but not a conviction. If the basis for the forfeiture is facilitation proceeds, the Government of Greece need not prove that the property was purchased with narcotics-related proceeds. The GOG must only demonstrate that it was used in furtherance of narcotics trafficking. Even legitimate businesses can be seized if they have laundered narcotics money.

Under Law 3691/2008, Greece has created a Strategic Committee to set national AML/CTF strategy and a Consultative Forum to ensure coordination with the private sector; and designated the MoEF as Central Coordination Authority to assess overall effectiveness.

Law 3691/2008 stipulates that terrorism financing is both a stand-alone offense and a predicate offense for money laundering. An amendment of the penal code extends the scope of terrorist financing to include individual terrorist acts and individual terrorists. The new law does not require that a terrorist act actually occur or that funding be used to finance a particular act, only that funds be used to finance terrorist organizations or groups, or individual terrorists or terrorist acts. Conviction for a terrorist financing offense carries a punishment of at least 10 years imprisonment and a fine of up to 2 million euros ($2.61 million). In the past, the Government of Greece had not provided guidance to obliged institutions on freezing assets without delay and has not monitored compliance with requests. There had been no sanctions for failure to follow freezing requests, and the traditional process for freezing or confiscating funds was lengthy. The new AML/CTF law authorizes the Minister of Economy and Finance to issue a ministerial decision for the freezing of assets of persons or entities suspected of terrorist financing, including those designated on the United Nations Security Council Resolution (UNSCR) 1267 Sanctions Committee consolidated list. The BOG has circulated to all financial institutions under its supervisory jurisdiction the list of individuals and entities on the UNSCR 1267 list, and regularly circulates updated lists as well as information related to financial provisions of UNSCRs related to Iran, the U.S. Treasury's Office of Foreign Asset Control (OFAC) lists, and U.S. Executive Order lists.

Greece exchanges information on money laundering through its mutual legal assistance treaty (MLAT) with the United States, which entered into force November 20, 2001. The Bilateral Police Cooperation Protocol provides a mechanism for exchanging records with U.S. authorities in connection with investigations and proceedings related to narcotics trafficking, terrorism, and terrorist financing. Cooperation between the U.S. Drug Enforcement Administration and YPEE has been extensive. Greece has signed bilateral police cooperation agreements with twenty countries, including the United States. It also has a trilateral police cooperation agreement with Bulgaria and Romania, and a bilateral agreement with Ukraine to combat terrorism, drug trafficking, organized crime, and other criminal activities. Despite the existing mechanisms for information exchange, the 2007 MER highlighted a lack of cooperation between Greek national and international authorities.

Greece is a party to the 1988 UN Drug Convention, the UN Convention Against Corruption, and the UN Convention for the Suppression of the Financing of Terrorism. Greece has signed, but not yet ratified the UN Convention against Transnational Organized Crime. Greece is a member of the FATF. Its FIU is a member of the Egmont Group.

The Government of Greece made many significant improvements to its AML/CTF regime in 2008, the results and implementation of which remain to be seen. In order to further enhance the effectiveness of its AML/CTF regime, Greece should continue to improve its FIU by making available further resources to deal with the STR backlog, as well as investigations, asset freezing and other actions the Commission is obligated to take. Greece should ensure that the FIU gets the necessary funding and training to develop an improved data management system capable of meeting the needs of the FIU to input, cross compare, and generally conduct a full analysis and possible investigation of all cases related to money laundering and terrorist financing. This includes improving its technical standards

and capabilities so that analysts can effectively use its database. These technological upgrades should allow Greek authorities to implement a system to track statistics on money laundering prosecutions, convictions, and sentences, as well as asset freezes and forfeitures. In addition, Greece should dedicate additional resources to the investigation and prosecution of ML cases, and increase specialization and training on AML/CTF for law enforcement and judicial authorities

Greece should issue clear guidance to supervised entities on the sanctions associated with breaches of and noncompliance with requirements under the new AML/CTF law. Authorities should ensure adequate regulation and supervision of lawyers, notaries, and nonprofits. Greece should issue clear guidance to financial institutions and DNFBPs on freezing assets; improve their asset freezing capabilities, and develop a clear and effective system for identifying and freezing terrorist assets. Greece should publicize its system for appealing assets frozen in accordance with its UN obligations. Greece should also ensure uniform enforcement of its cross-border currency reporting requirements and take further steps to deter the smuggling of currency across its borders; and explicitly abolish company-issued bearer shares. Greece also should ensure that companies operating within its free trade zones are subject to the same AML/CTF requirements and gatekeeper and due diligence provisions as in other sectors and bring charitable and nonprofit organizations under the AML/CTF regime. Finally, Greece should ratify the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Grenada

Grenada is not a regional financial center. As a transit location, money laundering in Grenada is primarily related to smuggling and drug-trafficking. Illicit proceeds are typically laundered through a wide variety of businesses, as well as through the purchase of real estate, boats, jewelry, and cars.

As of November 2008, Grenada's domestic financial sector is comprised of 26 registered domestic insurance companies, 12 credit unions, and five money remitters. Grenada has one trust company and 1,580 international business companies (IBCs), the same number as 2007, a significant, if unexplained, decrease from the 6,000 IBCs reported in 2006. There is one International Betting Company licensed to conduct business in Grenada, but no casinos or Internet gaming sites in operation. There are no free trade zones in Grenada, although the Government of Grenada (GOG) has indicated it may create one in the future. The GOG has repealed its economic citizenship legislation. In 2008, the GOG announced plans to redevelop an offshore financial sector. Grenada's previous offshore regime collapsed after a multimillion-dollar fraud scheme and its 2001 listing as a Non-Cooperative Country or Territory (NCCT) by the Financial Action Task Force (FATF). After enacting money laundering legislation and regulations in accordance with international standards, Grenada was removed from the NCCT list in 2003.

Bearer shares are not permitted for offshore banks. Registered agents are required by law to verify the identity of the beneficial owners of all shares. In addition, the International Companies Act requires registered agents to maintain records of the names and addresses of company directors and beneficial owners of all shares. Failure to maintain records may result in a penalty of $11,500 and possible revocation of the registered agent's license. There is no legal barrier to disclosure of client and ownership information by domestic and offshore services companies to bank supervisors and law enforcement authorities.

The Money Laundering Prevention Act (MLPA), enacted in 1999, and the Proceeds of Crime Act No. 3 (POCA) of 2003 criminalize money laundering in Grenada. Under the MLPA, the laundering of the proceeds of narcotics-trafficking and all serious crimes is an offense. Under the POCA, the predicate offenses for money laundering extend to all criminal conduct, which includes illicit drug and weapons trafficking, kidnapping, extortion, corruption, terrorism and its financing, and fraud. According to the POCA, no conviction on a predicate offense is required to prove that certain goods are the proceeds of

crime, or to subsequently convict a person for laundering those proceeds. The POCA establishes a penalty of three to ten years in prison and fines of $18,500 or more. This legislation applies to banks and nonbank financial institutions, as well as the offshore sector.

The Grenada Authority for the Regulation of Financial Institutions (GARFIN) became operational in 2007. The GARFIN was created to consolidate supervision of all nonbank financial institutions, and effectively replace the Grenada International Financial Services Authority (GIFSA). Institutions supervised by GARFIN include insurance companies, credit unions, offshore financial services, the building and loan society, money service businesses, and other such services. The Eastern Caribbean Central Bank (ECCB) retains supervision responsibility for Grenada's commercial banks.

Established under the MLPA, the Supervisory Authority supervises the anti-money laundering/counterterrorist financing compliance of banks and nonbank financial institutions (including money remitters, stock exchange, insurance, casinos, precious gem dealers, real estate intermediaries, lawyers, notaries, and accountants). These institutions are required to know, record, and report the identity of customers engaging in significant transactions, those over the threshold of $3,700. Records must be maintained for seven years. In addition, a reporting entity must monitor all complex, unusual or large business transactions, or unusual patterns of transactions, whether completed or not. Once a transaction is determined to be suspicious or potentially indicative of money laundering, the reporting entity must forward a suspicious transaction report (STR) to the Supervisory Authority within 14 days. Reporting individuals are protected by law with respect to their cooperation with law enforcement entities.

The Supervisory Authority issued its Anti-Money Laundering Guidelines in 2001. The guidelines direct financial institutions to maintain records, train staff, identify suspicious transactions, and designate reporting officers. The guidelines also provide examples to help institutions recognize and report suspicious transactions. The Supervisory Authority is authorized to conduct anti-money laundering inspections and investigations. The Supervisory Authority can also conduct investigations and inquiries on behalf of foreign counterparts and provide corresponding information. Financial institutions may be fined for not granting access to Supervisory Authority personnel.

The GOG regulates the cross-border movement of currency. However, there is no threshold requirement for currency reporting. Law enforcement and Customs officers have the powers to seize and detain cash that is imported or exported from Grenada. Cash seizure reports are shared among government agencies, particularly between Customs and the FIU.

In June 2001, the GOG established a police-style financial intelligence unit (FIU). The FIU is charged with receiving and analyzing STRs from the Supervisory Authority, and with investigating alleged money laundering offenses. The FIU has access to the records and databases of all government entities and financial institutions and is empowered to request any documents it considers necessary to its investigations. From January to November 2008, the FIU received 40 STRs and investigations commenced for all STRs received. The FIU has the authority to exchange information with its foreign counterparts without a memorandum of understanding (MOU).

Two foreign nationals were arrested by GOG authorities for money laundering in October 2007. These individuals came to Grenada with a large number of fraudulent credit cards and over a short period of time, withdrew in excess of $40,000 from automatic teller machines (ATMs) from several local banks. Half of the amount stolen was sent out to a number of different destinations via a legitimate money remittance company, which agreed to freeze the transaction. Local authorities are working with the company to repatriate those funds. The two perpetrators were arrested and charged with money laundering and fraud by false pretense. The women served one year in prison and were deported.

The FIU and the Director of Public Prosecution's Office are responsible for tracing, seizing and freezing assets. Under current law, all assets can be seized, including legitimate businesses if they are

used in the commission of a crime. The banking community cooperates with law enforcement efforts to trace funds and seize or freeze bank accounts. The time period for restraint of property is determined by the High Court. Presently, only criminal forfeiture is allowed by law. Proceeds from asset seizures and forfeitures can either be placed in the consolidated fund or the confiscated asset fund, which is supervised by the Supervisory Authority or the Cabinet for use in the development of law enforcement. No assets were seized in 2008. The approximate amount seized in 2007 was $62,000, with approximately $22,000 forfeited. The Civil Forfeiture Bill, Cash Forfeiture Act, and Confiscation of the Proceeds of Crime Bill were introduced in 2006 and remain under discussion.

Grenada is not a party to any bilateral or multilateral agreements to enhance asset tracing, freezing, and seizure. However, the GOG works actively with other governments to ensure traces, freezes, and seizures take place, if and when necessary, regardless of the status of existing agreements.

The GOG criminalizes terrorist financing through the Terrorism Act No. 5 2003. Grenada has the authority to identify, freeze, seize, and/or forfeit terrorist finance-related assets under the POCA and the Terrorism Act. The GOG circulates to the appropriate institutions the lists of individuals and entities included on the UN 1267 Sanctions Committee's consolidated list. There has been no known evidence of terrorist financing in Grenada. It is suspected alternative remittance systems are used in Grenada, though none have been positively identified.

In 2003, the GOG passed the Exchange of Information Act No. 2, which strengthens Grenada's ability to share information with foreign regulators. Grenada has a Mutual Legal Assistance Treaty (MLAT), Tax Information Exchange Agreement and Extradition Treaty with the United States. The GOG cooperates fully with MLAT requests and responds rapidly to U.S. Government requests for information involving money laundering cases.

Grenada is a member of the Caribbean Financial Action Task Force, a FATF-style regional body, and is scheduled to undergo a mutual evaluation in 2009. The GOG is also a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Grenada's FIU is a member of the Egmont Group. Grenada is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Grenada is not a party to the UN Convention against Corruption.

Although the Government of Grenada has strengthened the regulation and oversight of its financial sector, it will need to remain alert to potential abuses and steadfastly implement the laws and regulations it has adopted. The GOG should adopt its pending forfeiture and confiscation bills and establish mechanisms to identify and regulate alternative remittance systems. It should also establish large currency transaction reporting requirements governing financial institutions and border declarations. To improve the conduct of money laundering investigations, the FIU should improve coordination with other law enforcement bodies. The GOG should take advantage of opportunities for law enforcement and customs authorities to initiate money laundering investigations targeted on regional smuggling. To strengthen its legal framework against money laundering, Grenada should move expeditiously to become a party to the UN Convention against Corruption and should not redevelop its offshore financial sector.

Guatemala

Guatemala is a major transit country for illegal narcotics from South America and precursor chemicals from Europe and Asia. According to law enforcement agencies, narcotics trafficking and corruption are the primary sources of money laundered in Guatemala; however, the laundering of proceeds from other illicit activities, such as human trafficking, contraband, kidnapping, tax evasion, and vehicle theft, is substantial. Officials of the Government of Guatemala (GOG) believe that the sources of the

criminal proceeds laundered in Guatemala are derived from both domestic sources and foreign criminal activities. Mexican drug traffickers are increasing both their presence in the country and violent clashes with Guatemalan gangs. GOG officials also believe that cash couriers, offshore accounts, and wire transfers are used to launder funds, which are subsequently invested in real estate, small farms, capital goods, large commercial projects, and shell companies, or are otherwise transferred through the financial system. Guatemala continues to be a placement destination for bulk cash and lacks both legal resources and the expertise necessary to aggressively combat financial crime. Over the past year and a half, it is estimated that at least $60 million in drug-related proceeds have either been brought to or generated in Guatemala City. In 2008, approximately $4.32 billion in both formal and informal remittances were sent to Guatemala; a 4.6 percent increase over the total of $4.13 billion in 2007. Remittances sent from abroad account for approximately nine percent of Guatemala's gross domestic product. The vulnerabilities of historically weak law enforcement and judicial regimes, corruption, and increasing organized crime activity, contribute to a favorable climate for significant money laundering in Guatemala.

Guatemala is not considered a regional financial center, but it is an offshore center. Exchange controls have been lifted and dollar accounts are common, but some larger banks conduct significant business through their offshore subsidiaries. The Guatemalan financial services industry is comprised of 21 commercial banks; nine offshore banks, all of which are affiliated, as required by law, with a domestic financial group (including credit card, insurance, finance, commercial banking, leasing, and related subsidiaries); two licensed money exchangers; 26 money remitters, including wire remitters and remittance-targeting courier services; 17 insurance companies; 16 financial societies; 15 bonded warehouses; 244 savings and loan cooperatives; 11 credit card issuers; nine leasing entities; 11 financial guarantors; and one check-clearing entity operated by the Central Bank. There are also hundreds of unlicensed money exchangers that exist informally.

The Superintendence of Banks (SIB), which is directed by the Monetary Board, has oversight and inspection authority over the Central Bank (Bank of Guatemala), as well as over banks, credit institutions, financial enterprises, securities entities, insurance companies, currency exchange houses and other institutions as may be designated by the Bank of Guatemala Act. Guatemala's relatively small free trade zones target regional "maquila" (assembly line industry) and logistic center operations, and are not considered by GOG officials to be a major money laundering concern, although some proceeds from tax-related contraband may be laundered through them. The Ministry of Economy reviews and approves applications for companies to open facilities in free trade zones and confirms their business operations meet legal requirements.

The offshore financial sector initially offered a way to circumvent currency controls and other costly financial regulations. However, financial sector liberalization largely removed incentives for legitimate businesses to conduct offshore operations. All offshore institutions are currently subject to the same requirements as onshore institutions and are regulated by the SIB. In June 2002, Guatemala enacted the Banks and Financial Groups Law (No. 19-2002), which placed offshore banks under the oversight of the SIB. The law requires offshore banks that belong to a Guatemalan financial group to be authorized by the Monetary Board and to maintain an affiliation with a domestic institution. It also prohibits an offshore bank that is authorized in Guatemala from conducting financial intermediation activities in another jurisdiction. Banks authorized by other jurisdictions may do business in Guatemala under certain limited conditions.

Pursuant to a 2003 resolution of the Monetary Board, an offshore bank can be authorized, only if the financial group to which it belongs has been previously authorized. By law, no offshore financial services businesses, other than banks, are allowed. In 2004, the SIB and Guatemala's financial intelligence unit (FIU), the Intendencia de Verificación Especial (IVE), concluded a process of reviewing and licensing all offshore entities, which resulted in the closure of two operations. No offshore trusts have been authorized. Offshore casinos and Internet gaming sites are not regulated.

There is continuing concern over the volume of money passing informally through Guatemala. Much of the more than $4.32 billion in 2008 remittance flows (97.7 percent from the U.S.) passed through informal channels, although sector reforms led to an increased use of banks and other formal means of transmission. Terrorist finance legislation enacted in August 2005 requires remitters to maintain name and address information on senders (97 percent U. S. based) of transfers equal to or over an amount to be determined by implementing regulations that will be in place by 2009. Increasing financial sector competition should continue to expand services and bring more people into the formal banking sector, helping to further isolate those who abuse informal channels.

Decree 67-2001, or the "Law Against Money and Asset Laundering," criminalizes money laundering in Guatemala. This law specifies that individuals convicted of money or asset laundering are subject to a noncommutable prison term ranging from six to 20 years, and fines equal to the value of the assets, instruments or products resulting from the crime. Convicted foreigners are deported from Guatemala. Conspiracy and attempt to commit money laundering are also penalized. The law applies to money laundering from any crime and does not require a minimum threshold to be invoked. It also holds institutions and individuals responsible for failure to prevent money laundering or allowing money laundering to occur, regardless of personal culpability. Banks and financial institutions can lose their banking licenses; and the institutions, directors, and other employees may face criminal charges if they are found guilty of failure to prevent money laundering. This law also applies to offshore entities that operate in Guatemala but are registered under the laws of another jurisdiction.

Decree 67-2001 also obligates individuals to declare the cross-border movement of currency in excess of approximately $10,000 at the ports of entry. The declaration forms are provided and collected by the tax authority at land borders, airports, and ports. The tax authority sends a copy of the sworn declaration to IVE for its database. The IVE can share this information with other countries under the terms and conditions specified by mutual agreement. In addition, the Law Against the Financing of Terrorism penalizes the omission of declaration with a sentence from one to three years in prison. At Guatemala City's international airport, a special unit was formed in 2003 to enforce the use of customs declarations upon entry to and exit from Guatemala. Approximately $4.1 million has been seized at the airports, as of October 2008—suggesting that proceeds from illicit activity are regularly hand-carried over Guatemalan borders. However, apart from a cursory check of a self-reporting customs form and random searches, there is little monitoring of compliance at the airport. Compliance is not regularly monitored at land borders. Further complicating compliance is the Central American Four Agreement, which allows free movement of the citizens of Guatemala, Honduras, Nicaragua, and El Salvador across their respective borders.

In addition to the requirements of Decree 67-2001, the Guatemalan Monetary Board's Resolution JM-191, which approved the "Regulation to Prevent and Detect the Laundering of Assets" (RPDLA), established anti-money laundering requirements for financial institutions. The RPDLA required all financial institutions under the oversight and inspection of the SIB to establish anti-money laundering measures, and introduced requirements for transaction reporting and record keeping. The Guatemalan financial sector has largely complied with these requirements and has a generally cooperative relationship with the SIB.

Financial institutions are prohibited from maintaining anonymous accounts or accounts that appear under fictitious or inexact names. Nonbank financial institutions and privately held companies, however, may issue bearer shares to their partners and stockholders thereby protecting the identity of the owners from public disclosure. However, Guatemalan law prohibits the issuance of bearer shares or privacy laws from being used to prevent the disclosure of financial information to bank supervisors and law enforcement authorities. Financial institutions are required to keep a registry of their customers as well as some types of transactions, such as the opening of new accounts or the leasing of safety deposit boxes. Financial institutions must also keep records of the execution of cash transactions exceeding $10,000 or more per day, and report these transactions to the IVE. Under

Decree 67-2001, financial institutions must maintain records of these registries and transactions for five years. Financial institutions are also mandated by law to report all suspicious transactions to the IVE. The law also exonerates financial institutions and their employees of any criminal, civil or administrative penalty for their cooperation with law enforcement and supervisory authorities with regard to the information they provide.

Decree 67-2001 established the IVE within the Superintendence of Banks to supervise financial institutions and ensure their compliance with the law. The IVE began operations in 2002 and in 2008 had a staff of 44. The IVE has the authority to obtain all information related to financial, commercial, or business transactions that may be connected to money laundering. The IVE conducts inspections of financial institution management, compliance officers, anti-money laundering training programs, "know-your-client" policies, and auditing programs. From January 2001 to October 2008, the IVE imposed over $125,000 in administrative penalties for institutional failure to comply with anti-money laundering regulations. As of October 2008, approximately $70,000 in assessed fines was pending final resolution.

In 2008, the IVE underwent an internal reorganization to improve its efficiency and coordination with the Public Ministry and courts. Four new sections were created, the first of which focuses on risk evaluation and prevention through examination of rules, working with banks, and strengthening the reporting of suspicious transactions. The second unit centers on investigating suspicious transactions. The third unit focuses on coordinating directly with the Public Ministry and courts to ensure they have all of the information required as well as provide the IVE with a means to track the status of cases. The fourth unit focuses on analyzing money laundering trends and best practices.

Since its inception, the IVE has received approximately 2,595 suspicious transaction reports (STRs), 293 from January to October 2008, from the 419 obligated entities in Guatemala. All STRs are received electronically, and the IVE has developed a system of prioritizing them for analysis. After determining that an STR is highly suspicious, the IVE gathers further information from public records and databases, other covered entities and foreign FIUs, and assembles a case. Once the IVE has determined a case warrants further investigation, the case must receive the approval of the SIB before being sent to the Anti-Money or Other Assets Laundering Unit (AML Unit) within the Public Ministry. Under current regulations, the IVE cannot directly share the information it provides to the AML Unit with any other special prosecutors (principally the anticorruption or counternarcotics units) in the Public Ministry but the AML Unit may request the Attorney General authorize the transfer of a case to another prosecutor given the nature of the crime. The IVE also assists the Public Ministry by providing information upon request for other cases the prosecutors are investigating.

The AML Unit in the Public Ministry is in charge of directing the investigation and prosecution of money laundering cases. This unit has a staff of 14 officials, and an investigative support group of eight law enforcement officers and investigators. Both the prosecutors and investigators receive yearly ad hoc training in various investigative and legal issues. The IVE referred 12 complaints and two reports to the AML Unit as of October 2008. The Public Ministry's AML Unit initiated 47 cases as of January 2007, one of which was transferred to another prosecutor for investigation and prosecution due to the nature of the particular crime. Twenty-four money laundering prosecutions have been concluded, 23 of which resulted in convictions. In several cases, assets have been frozen. The cases were made possible by information supplied by cooperating financial institutions. No reports or cases of terrorist financing were reported in 2008 by the IVE.

In 2006, Guatemala created a money laundering task force. The money laundering task force is a joint unit comprised of individuals from the Guatemalan Tax Authority (SAT), the IVE, Public Ministry's AML Prosecutor's Office, and Ministry of Government's National Civil Police. Together they work on investigating financial crimes, building evidence and bringing cases to prosecution. In 2008, the

task force was working on four major money laundering investigations and a number of significant drug-related cases.

Current law permits the seizure of any assets linked to money laundering. The IVE, the National Civil Police, and the Public Ministry have the authority to trace assets; the Public Ministry can seize assets temporarily in urgent circumstances, and only the Courts of Justice have the authority to permanently seize assets. In 2003, the Guatemalan Congress approved reforms to allow seized money to be shared among several GOG agencies, including police and the IVE. Nevertheless, the Constitutional Court ruled that all forfeited currency remains under the jurisdiction of the Supreme Court of Justice. The courts do not allow seized currency to be used by enforcement agencies while cases remain open. For money laundering and narcotics cases, any seized money is deposited in a bank safe and all material evidence is sent to the warehouse of the Public Ministry. There is no central tracking system for seized assets, and it is currently impossible for the GOG to provide an accurate listing of the seized assets in custody. In 2008, the Public Ministry reported $3.4 million in seized cash. The lack of access to the resources of seized assets outside of the judiciary has made sustaining seizure levels difficult for the resource-strapped enforcement agencies.

In 2006, Guatemala passed an Anti-Organized Crime Law. Under the law, the use of undercover operations, controlled deliveries, and wire taps is permitted to investigate many forms of organized crime activity, including money laundering crimes. The Anti-Organized Crime Law also provides the possibility for a summary procedure to forfeit the seized assets and allows both civil and criminal forfeiture. Implementing regulations have been enacted, however, the Public Ministry and National Civil Police have not yet set up the units to execute undercover operations, controlled deliveries and wire intercepts.

Guatemala has made significant progress in the implementation of the Financial Action Task Force (FATF) Special Recommendations I, II and V on Terrorist Financing since its last Mutual Evaluation in 2005 by the Caribbean Financial Action Task Force (CFATF), a FATF-style regional body. In June 2005, the Guatemalan Congress passed legislation criminalizing terrorist financing, the “Law Against the Financing of Terrorism.” Implementing regulations were enacted by the Monetary Board in December 2005. The counterterrorist financing legislation also clarified the legality of freezing assets in the absence of a conviction where the assets were destined to support terrorists or terrorist acts. The legislation brings Guatemala into compliance with the FATF Special Recommendations on Terrorist Financing and the United Nations (UN) Security Council Resolution 1373. The GOG has fully cooperated with U.S. efforts to track terrorist financing funds and distributes the UN 1267 sanctions committee’s consolidated list of entities linked to Usama Bin Ladin, al Qaida and the Taliban to Guatemalan financial institutions.

Guatemala is a party to the UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. The GOG is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force. In 2003, the IVE became a member of the Egmont Group. The IVE has signed a number of Memoranda of Understanding regarding the exchange of information on money laundering issues, seventeen of which also include the exchange of information regarding the financing of terrorism.

Corruption and organized crime remain endemic in Guatemala and are the biggest long-term challenges to the rule of law in Guatemala. The Government of Guatemala has made efforts to comply with international standards and improve its anti-money laundering and counterterrorist financing regime; however, Guatemala should eliminate the use of bearer shares and regulate offshore gaming and casino establishments. The GOG should also continue efforts to improve enforcement of existing regulations, establish units to execute operations authorized in the Anti-Organized Crime Law, and

pursue much needed reforms in the law enforcement and justice systems. Cooperation between the IVE and the Public Ministry has improved in recent years, and several investigations have led to prosecutions. Guatemala should increase its capacity to successfully investigate and prosecute money laundering cases. Additionally, the GOG should create an asset forfeiture fund and a centralized agency to manage and dispose of seized and forfeited assets to law enforcement agencies that will provide the Government with the resources necessary in the fight against money laundering, terrorist financing, and other financial crimes. In addition, the GOG should enhance its pursuit of confiscation and forfeiture of the proceeds of arms smuggling, human trafficking, corruption, and other organized criminal activities, and should enact domestic laws permitting international sharing of confiscated assets.

Guernsey

The Bailiwick of Guernsey (the Bailiwick) encompasses a number of the Channel Islands (Guernsey, Alderney, Sark, and Herm). As a Crown Dependency of the United Kingdom (UK), it relies on the UK for its defense and international relations; however, the Bailiwick is not part of the UK. Alderney and Sark have their own separate parliaments and civil law systems. Guernsey's parliament legislates criminal justice matters for all of the islands in the Bailiwick. Guernsey is a sophisticated financial center and, as such, continues to be vulnerable to money laundering at the layering and integration stages.

The approximately 18,800 companies registered in the Bailiwick do not fall within the standard definition of an international business company (IBC). Guernsey and Alderney incorporate companies, but Sark, which has no company legislation, does not. Companies in Guernsey must disclose beneficial ownership to the Guernsey Financial Services Commission (FSC) before legal formation or acquisition.

Guernsey has 48 licensed banks, all of which have offices, records, and a substantial presence in the Bailiwick. The banks are licensed to conduct business with residents and nonresidents alike. There are approximately 714 international insurance companies and 829 collective investment funds. There are also approximately 18 bureaux de change, ten of which are part of a licensed bank. Bureaux de change and other money service providers must register with the FSC.

Guernsey has a comprehensive legal framework to anti-money laundering and counterterrorist financing. The original 1999 anti-money laundering law creates a system of suspicious transaction reporting, including suspicion of tax evasion. Suspicious transaction reports (STRs) are sent to the Financial Intelligence Service (FIS), Guernsey's financial intelligence unit (FIU). Guernsey further honed its anti-money laundering/counterterrorist financing (AML/CTF) legislation with the Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) Regulations, 2007. The legislation criminalizes money laundering for all crimes except drug-trafficking, which the Drug Trafficking (Bailiwick of Guernsey) Law, 2000, as amended, covers in identical terms. The Disclosure (Bailiwick of Guernsey) Law 2007 makes failure to disclose the knowledge or suspicion of money laundering a criminal offense. The duty to disclose suspicious activity extends to all businesses, not only financial services businesses. In 2007, the FSC issued companion guidance entitled "Handbook for Financial Services Businesses on Countering Financial Crime and Terrorist Financing" which replaces the Guidance Notes on the Prevention of Money Laundering and Countering the Financing of Terrorism.

Guernsey's legal framework contains additional legislative provisions aimed at assisting in the detection of money laundering and terrorist financing. These include search and seizure powers, customer information orders and account monitoring orders. The Transfer of Funds (Guernsey) Ordinance 2007 requires any parties that offer funds transfer services to obtain verified identification information for any person transferring funds electronically.

Guernsey authorities approved further measures to strengthen the existing AML/CTF regime with the passage of numerous legislation, regulations, and ordinances in 2008. These include a comprehensive civil forfeiture law, new regulations for certain entities involved in high value transactions, and legislation governing charities and other nonprofit organizations.

Guernsey enacted the Prevention of Corruption (Bailiwick of Guernsey) Law of 2003 and the Regulation of Fiduciaries, Administration Businesses, and Company Directors, etc. (Bailiwick of Guernsey) Law of 2000 ("the Fiduciary Law") to license, regulate and supervise company and trust service providers. Pursuant to Section 35 of the Fiduciary Law, the FSC must license all fiduciaries, corporate service providers and persons acting as company directors on behalf of any business. The FSC creates Codes of Practice for corporate service providers, trust service providers, and company directors. To receive licenses, these agencies must follow strict standards, including client identification and "know your customer" (KYC) requirements. These entities are subject to regular inspection, and an entity's failure to comply could result in prosecution and revocation of its license. The Bailiwick is fully compliant with the Offshore Group of Banking Supervisors (OGBS) Statement of Best Practice for Company and Trust Service Providers.

The FSC regulates the Bailiwick's banks, insurance companies, mutual funds and other collective investment schemes, investment firms, fiduciaries, company administrators and company directors. The Bailiwick does not permit bank accounts to be opened unless there has been a KYC inquiry and the customer provides verification details. Regulations contain penalties to be applied when financial services businesses do not follow their obligations. Upon a company's application for incorporation, the FSC evaluates the request. The Royal Court maintains the registry of incorporated companies. The Court will not permit incorporation unless the FSC and the Attorney General or Solicitor General have given approval. The FSC conducts regular on-site inspections and analyzes the accounts of all regulated institutions.

As mandated in the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law, 1999, as amended, the FSC has a public register of money service providers, including money brokerage firms, money changers, and any business that facilitates or transmits money or value through an informal money or value transfer system or network. Not all financial services businesses are licensed under the Proceeds of Crime Law, as amended. Businesses not licensed under the above legislation must be registered under the Registration of Non-Regulated Financial Services Businesses (Bailiwick of Guernsey) Law, 2008, as amended. This legislation creates a public register of nonregulated financial services businesses which the FSC maintains on its website. Applications for registration must be made to the FSC. The FSC has no obligation to make any enquiries concerning an application for registration or the continued registration of any nonregulated financial services business, unless there is a notice regarding the grounds whereby it could refuse or revoke an application or registration of such a business.

On July 1, 2005, the European Union Savings Tax Directive (ESD) came into force. The ESD is an agreement between the Member States of the European Union (EU) to automatically exchange information with other Member States about EU tax resident individuals who earn income in one EU Member State but reside in another. Although not part of the EU, the three UK Crown Dependencies (Guernsey, Jersey, and the Isle of Man) have voluntarily agreed to apply the same measures to those in the ESD and have elected to implement the withholding tax option—also known as the "retention tax option"—within the Crown Dependencies.

The Guernsey authorities have established a forum, the Crown Dependencies Anti-Money Laundering Group, where the Attorneys General, Directors General, and representatives of Police, Customs, the regulatory community and FIUs from the Crown Dependencies meet to coordinate AML/CTF policies and strategy.

The FIS operates as the Bailiwick's FIU, and is comprised of Police and Customs Officers. The Service Authority, a committee of senior Police and Customs Officers who coordinate the Bailiwick's financial crime strategy, directs the FIS. With a mandate to focus on money laundering and terrorist financing issues, the FIS serves as the central point within the Bailiwick for the receipt, collation, analysis, and dissemination of all financial crime intelligence, much of which comes from STR filings. In 2007, the FIS received 539 STRs.

An IMF assessment is scheduled to take place in Guernsey in late 2009. The assessment will cover banking, insurance and investment sector supervisory legislation and practice, together with AML/CTF legislation and its implementation.

There has been counterterrorism legislation covering the Bailiwick since 1974. The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002, replicates equivalent UK legislation. The Terrorism Law criminalizes the failure to report suspicion or knowledge of terrorist financing.

Through the Bailiwick narcotics trafficking, money laundering, and terrorism laws, enforcement of foreign restraint and confiscation orders apply to those foreign countries designated by the UK.

Guernsey cooperates with international law enforcement on money laundering cases. The FSC also cooperates with regulatory/supervisory and law enforcement bodies. The Criminal Justice (International Cooperation) (Bailiwick of Guernsey) Law, 2000 furthers cooperation between Guernsey and other jurisdictions by allowing certain investigative information concerning financial transactions to be exchanged. In cases of serious or complex fraud, Guernsey's Attorney General can provide assistance under the Criminal Justice (Fraud Investigation) (Bailiwick of Guernsey) Law 1991.

On September 19, 2002, the United States and Guernsey signed a Tax Information Exchange Agreement, which came fully into force in 2006. The agreement provides for the exchange of information on a variety of tax investigations, paving the way for audits that could uncover tax evasion or money laundering activities. Guernsey is negotiating similar agreements with other countries. The 1988 U.S.-UK Agreement Concerning the Investigation of Drug Trafficking Offenses and the Seizure and Forfeiture of Proceeds and Instrumentalities of Drug Trafficking, as amended in 1994, was extended to the Bailiwick in 1996.

Upon its extension to the Bailiwick in 2002, Guernsey enacted the necessary legislation to implement the 1988 UN Drug Convention. The Bailiwick has requested the UK Government seek the extension to the Bailiwick of the UN Convention for the Suppression of the Financing of Terrorism.

Guernsey is a member of the Offshore Group of Insurance Supervisors and the Offshore Group of Banking Supervisors. The FIS is a member of the Egmont Group and represents the jurisdiction within The Camden Assets Recovery Inter-Agency Network (CARIN), an informal network of EU member state contacts convened to work on asset recovery.

Guernsey should continue to amend its legislation to meet international AML/CTF standards and should ensure complete implementation of its new 2008 legislation. It should integrate civil forfeiture into its legal framework. Guernsey should also take steps to ensure the obliged entities uphold their legal obligations, and the regulatory authorities have the tools they need to provide supervisory functions, especially with regard to nonfinancial businesses and professions not currently regulated. Guernsey should likewise fully implement UNSCRs 1267 and 1373 and ensure all obliged entities receive the UN 1267 Sanctions Committee's consolidated list of entities and individuals.

Guinea-Bissau

Guinea-Bissau is not a regional financial center. Increased drug trafficking and the prospect of oil production, increase its vulnerability to money laundering and financial crime. Drug traffickers

transiting between Latin America and Europe have increased their use of the country. Guinea-Bissau is often the placement point for proceeds from drug payoffs, theft of foreign aid, and corrupt diversion of oil and other state resources headed for investment abroad. A recent boom in the construction of luxury homes, hotels and businesses, and the proliferation of expensive vehicles, stand in sharp contrast with the conditions in the poor local economy. It is likely that at least some of the new wealth derives from money laundered from drug trafficking. Banking officials also think the country is vulnerable to trade-based money laundering (TBML).

The legal basis for Guinea-Bissau's anti-money laundering/counterterrorist financing (AML/CTF) framework is the Loi Uniforme Relative a Lutte Contre le Blanchiment de Capiteaux No. 2004-09 of February 6, 2004, or the Anti-Money Laundering Uniform Law (Uniform Law). As the common law passed by the members of West African Economic and Monetary Union (WAEMU or UEMOA), all member states are required to enact and implement the legislation. On November 2, 2004, Guinea-Bissau became the third WAEMU/UEMOA country to enact the Uniform Law. The legislation largely meets international standards with respect to money laundering. Guinea-Bissau has an "all crimes" approach to money laundering. The law requires banks and other financial institutions to implement Know Your Customer (KYC) measures and to record and report the identity of any person who engages in significant transactions, including the recording of large currency transactions. Obliged institutions include financial institutions and nonbank financial institutions such as exchange houses, brokerages, cash couriers, casinos, insurance companies, charities, nongovernmental organizations (NGOs), and intermediaries such as lawyers, accountants, notaries and broker/dealers.

According to the law, obliged entities must report all suspicious transactions to the financial intelligence unit (FIU). There is no threshold amount triggering a report. Safe harbor provisions give reporting individuals and their supervisors civil and criminal immunity from professional sanctions for providing information to the FIU in good faith. The law also criminalizes self laundering. It is not necessary to have a conviction for the predicate offense before prosecuting or obtaining a conviction for money laundering. Criminal liability applies to all legal persons as well as natural persons. However, the legislation does not comply with all Financial Action Task Force (FATF) recommendations concerning politically-exposed persons (PEPs), and lacks certain compliance provisions for nonfinancial institutions. Article 26 of National Assembly Resolution No. 4 of 2004 stipulates that if a bank suspects money laundering it must obtain a declaration of all properties and assets from the subject and notify the Attorney General, who must then appoint a judge to investigate. Reportedly, banks are reluctant to file suspicious transaction reports (STRs) because of the fear of "tipping off" by an allegedly indiscrete judiciary. The bank's solicitation of an asset list from its client could also amount to "tipping off" the subject. The Central Bank of West African States (BCEAO), based in Dakar, is the Central Bank for the eight countries in the WAEMU, including Guinea-Bissau, and uses the CFA franc currency. The Commission Bancaire, the BCEAO division responsible for bank inspections, is based in Abidjan. However, it does not execute a full AML examination during its standard banking compliance examinations. All three banks operating in the country report that they have AML compliance programs in place

Western Union and MoneyGram function under the auspices of the banks. Unlicensed money remitters and currency exchangers, although prevalent, are illegal. Authorities report problems with porous borders and cash smuggling; reportedly, corruption in the Customs agency exacerbates this situation. Although the current AML legislation obliges NGOs and nonprofits, including charities, to file STRs, the current regulatory regime is unknown.

The 2004 Uniform Law provides for the establishment of an FIU, and the country issued a Directive in 2006 to establish its FIU. However, no operational FIU exists in the country. Guinea-Bissau is working with external donors to establish a functioning FIU, which will be housed within the Ministry of Economy and Finance. A senior Ministry of Finance official will administer the FIU. The FIU's mandate will be to receive and analyze STRs and, when appropriate, to refer files to the Prosecutor

General. The FIU will rely on counterparts in law enforcement and other governmental institutions to provide information upon request for the FIU's investigations. Lack of capacity, corruption, instability, and distrust (particularly of the judicial sector), could significantly hamper progress in the FIU's development. The FIU, when operational, will have the authority to share information with any other FIU in the WAEMU/UEMOA countries.

The Judicial Police and prosecutors investigate money laundering as well as terrorist financing. Two Judicial Police officers are currently undergoing training for investigations of money laundering and terrorist financing, and were expected to complete their training in January 2009. The Attorney General's office houses a small unit to investigate corruption and economic crimes. In November 2007, the Government of Guinea-Bissau's (GOGB) Audit Office created a commission to investigate illegal acquisition of wealth by present and former government officials. However, a lack of training and capacity, endemic corruption and a reported lack of cooperation from banks impede investigations. Official statistics regarding the prosecution of financial crimes are unavailable. There are no known prosecutions of money laundering. Despite the country's legal obligation as a WAEMU member state to fully implement the Uniform Law, Judicial Police officials have opined that the Uniform Law is unwieldy and inappropriate for Guinea-Bissau's environment. In 2008, no financial institutions reported any suspicious transactions, nor did authorities initiate any money laundering investigations.

Under Guinea-Bissau's law, money from assets seized in the course of a counternarcotics investigation should be applied to further counternarcotics efforts. However, the inability to agree upon which governmental department should be the beneficiary of the seized assets has resulted in the funds going to the state treasury. An inter-ministerial proposal to credit all drug-related seized assets to the Judicial Police was pending at the end of 2008.

The WAEMU/UEMOA Uniform Law does not deal with terrorist financing. Article 203, Title VI of Guinea-Bissau's penal code criminalizes terrorist financing. However, it has no reporting requirements or attendant regulations. In addition, because the penal code only criminalizes the financing of terrorist groups or organizations, it does not address financing of a single or individual terrorist. The penal code also does not criminalize the financing of terrorist organizations when the money is not used to commit terrorist acts. The BCEAO has released Directive No. 04/2007/CM/UEMOA, obliging member states to pass domestic counterterrorist financing (CTF) legislation. Member states must enact a law against terrorist financing, which will likely be a Uniform Law similar in form and obligation to the AML law. Each national assembly must then enact the law. In July 2007, UEMOA/WAEMU released attendant guidance on terrorist financing for member states. The FATF-style regional body to which Guinea-Bissau belongs, the African Anti-Money Laundering Inter-governmental Group (GIABA), has drafted a uniform law, which it has recommended to its member states for adoption.

The Ministry of Finance and the BCEAO circulate the UN 1267 Sanctions Committee consolidated list to commercial financial institutions. The WAEMU/UEMOA Council of Ministers has issued a directive requiring banks to freeze assets of entities designated by the Sanctions Committee. To date, no institution has identified assets relating to terrorist entities.

Multilateral ECOWAS treaties deal with extradition and legal assistance. Guinea-Bissau is a party to the 1988 UN Drug Convention, and has signed but not ratified the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention Against Corruption. Transparency International's 2007 Corruption Perception Index ranks Guinea Bissau 147 out of 180 countries.

The Government of Guinea-Bissau should continue to work with its partners in GIABA, WAEMU/UEMOA and ECOWAS to establish and implement a comprehensive AML/CTF regime that comports with all international standards. The GOGB should ensure that the sectors covered by its AML law have implementing regulations and competent authorities to ensure compliance with the

law's requirements. The GOGB should clarify, amend or eliminate Article 26 of the 2004 National Assembly Resolution that appears to mandate actions resulting in the tipping off of suspects. It should also adopt and enact a terrorist financing law. Guinea-Bissau should amend the definitions in its penal code to comport with the international standards regarding financing of individual terrorists and terrorist groups engaging in acts other than terrorism. It should establish, staff and train, its FIU, and ensure that resources are available to sustain its capacity. It should work to improve the training and capacity of its police and judiciary to combat financial crimes, and address any issues resulting from a lack of understanding of money laundering and terrorist financing. Guinea-Bissau should undertake efforts to eradicate systemic corruption and become a party to the UN Convention for the Suppression of the Financing of Terrorism, and the UN Conventions against Corruption and Transnational Organized Crime.

Guyana

Guyana is neither an important regional nor an offshore financial center, nor does it have any free trade zones. Money laundering is perceived as a serious problem, and has been linked to trafficking in drugs (principally cocaine) and firearms, as well as to corruption and fraud. Guyana has a large informal economy that is vulnerable to money laundering. The Government of Guyana (GOG) made no arrests or prosecutions for money laundering in 2008. Guyana currently has inadequate legal and enforcement mechanisms to combat money laundering, lacks enabling legislation to combat terrorist financing, and its financial intelligence unit (FIU) does not meet the membership requirements to join the Egmont Group.

Under the Money Laundering Prevention Act (MLPA) of 2000, money laundering is an autonomous crime. Although not dependent on the successful prosecution of a predicate crime, the MLPA narrowly defines money laundering as involving the proceeds of certain "prescribed offences," including blackmail, bribery, counterfeiting, drug trafficking and related offenses, false accounting, forgery, fraud, illegal deposit-taking, robbery involving more than $20,000, thefts involving more than $20,000, and insider trading. The MLPA does not cover the financing of terrorism or "all serious crimes" in its list of prescribed offenses. Banks, offshore banks, finance companies, currency exchange houses, insurance companies, money transmission services, factoring companies, leasing companies, trust companies, and securities and loan brokers are required to report suspicious transactions to the FIU, and records of suspicious transaction reports (STRs) must be kept for six years. Lawyers, casinos, notaries, and accountants are among those entities exempt from financial regulatory control.

Undeclared or misdeclared cross-border movement of currency exceeding $10,000 is a customs violation, subject to a $250,000 fine and six months in prison. Notably, such offenses are reported to the Customs Administration, but not to Guyana's FIU and other law enforcement bodies.

The Organization of American States reports that the GOG received 15 STRs in 2004, 53 in 2005, and 110 in 2006. GOG has reportedly not released statistics on the number of STRs received in 2007 or 2008 by the FIU, despite the suggestion that the FIU should make these statistics available to relevant authorities as recommended by the Financial Action Task Force (FATF). The MLPA establishes the Guyana Revenue Authority, the Customs Anti-Narcotics Unit, the Attorney General, the Director for Public Prosecutions, and the FIU as the authorities responsible for investigating financial crimes.

The GOG's anti-money laundering regime is rendered ineffective by other major structural weaknesses of the MLPA. While the MLPA provides for the seizure of assets derived as proceeds of crime, guidelines for implementing seizures and forfeitures have never been established. While the FIU may request additional information from obligated entities, it does not have access to law enforcement information or the authority to exchange information with its foreign counterparts. The FIU has also been staffed by only one person. These limitations collectively stifle the analytical and

investigative capabilities of the FIU and law enforcement agencies. As a result of these weaknesses, there has been no money laundering prosecutions or convictions to date.

To augment the tools available to the GOG's anti-money laundering authorities, in 2007 the FIU drafted legislation entitled the Anti-Money Laundering and Countering the Financing of Terrorism Bill. The bill provides for the identification, freezing, and seizure of proceeds of crime and terrorism; establishes comprehensive powers for the prosecution of money laundering, terrorist financing, and other financial crimes; requires reporting entities to take preventive measures to help combat money laundering and terrorist financing; provides for the civil forfeiture of assets; expands the scope of the money laundering offense; and mandates the accessibility of all relevant data among law enforcement agencies. The legislation provides for oversight of export industries, the insurance industry, real estate, and alternative remittance systems, and sets forth the penalties for noncompliance. The bill also establishes the FIU as an independent body that answers only to the President, and defines in detail its role and powers. The draft legislation was tabled in Parliament in late 2007, and remains in committee debate at the conclusion of 2008. Its passage in the near future is uncertain.

The GOG and the Bank of Guyana continue to assist U.S. efforts to combat terrorist financing by working toward compliance with relevant United Nations Security Council Resolutions (UNSCRs). In 2001, the Bank of Guyana, the sole financial regulator as designated by the Financial Institutions Act of March 1995, issued orders to all licensed financial institutions expressly instructing the freezing of all financial assets of terrorists, terrorist organizations, and individuals and entities associated with terrorists and their organizations. Guyana has no domestic laws authorizing the freezing of terrorist assets, but the government created a special committee on the implementation of UNSCRs, co-chaired by the Head of the Presidential Secretariat and the Director General of the Ministry of Foreign Affairs. To date the procedures have not been tested, as no terrorist assets have been identified in Guyana. The FIU director also disseminates the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list to relevant financial institutions.

Guyana is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force (CFATF). Guyana is a party to the UN 1988 Drug Convention and the UN Convention against Transnational Organized Crime. On April 16, 2008, Guyana acceded to the UN Convention against Corruption. Guyana's FIU is one of the few in the region that is not a member of the Egmont Group, and no change in that status is anticipated until Guyana's anti-money laundering laws have been modernized and the financing of terrorism is criminalized. Guyana does not have a Mutual Legal Assistance Treaty (MLAT) with the United States, but is a party to the Inter-American Convention on Mutual Legal Assistance.

The Government of Guyana should pass the draft legislation on money laundering and terrorist financing that is currently before the Parliament. Enactment of this legislation would extend preventive measures to a wider range of reporting entities, including casinos and designated nonfinancial businesses and professions (DNFBPs). The draft legislation would also provide greater resources and critical autonomy for the FIU, enable the FIU to access law enforcement data, and ensure that the FIU has the operational capacity to meet the membership requirements of the Egmont Group. In short, the passage of this legislation is essential in enhancing the GOG's compliance with international standards and ensuring that its anti-money laundering and counterterrorist financing regime is operational and effective. In the interim, Guyana should provide appropriate resources and awareness training to its regulatory, law enforcement, and prosecutorial personnel, and establish procedures for asset seizure and forfeiture.

Haiti

Haiti is not a major financial center. Haiti's dire economic condition and unstable political situation inhibit the country from advancing its formal financial sector. Haiti is a major drug-transit country with money laundering activity linked to the drug trade and to kidnapping. Rampant corruption of public officials also generates illicit proceeds. Money laundering and other financial crimes are facilitated through banks and casinos, as well as through foreign currency and real estate transactions. While the informal economy in Haiti is significant and partly funded by illicit narcotics proceeds, smuggling is historically prevalent and predates narcotics trafficking. Haiti's geo-strategic position, lack of an efficient judiciary system, uncontrolled borders, weak police force (about one police officer per 1,000 civilians), and corruption throughout the public sector exacerbate the favorable environment for money laundering.

The Government of Haiti (GOH) has made progress in recent years to improve its legal framework, create and strengthen core public institutions, and enhance financial management processes and procedures. The government of President Rene Preval has continued the monetary, fiscal and foreign exchange policies initiated under the past Interim Government of Haiti with the assistance of the International Monetary Fund and the World Bank. Continued insecurity and a lack of personnel expertise, however, have impacted the Government's initiatives and slowed its ability to modernize its regulatory and legal framework.

Since 2001, Haiti has used the Law on Money Laundering from Illicit Drug Trafficking and other Crimes and Punishable Offenses (AMLL) as its primary anti-money laundering legislation. The AMLL criminalizes money laundering and establishes a wide range of financial institutions as obligated entities, including banks, money remitters, exchange houses, casinos, and real estate agents. Insurance companies, which are only nominally represented in Haiti, are not covered. The AMLL regulations were amended in 2008 and require financial institutions to establish money laundering prevention programs and to verify the identity of customers who open accounts or conduct transactions that exceed 400,000 Gourde (HTG) (approximately $10,000). It also requires exchange brokers and money remitters compile information on the source of funds exceeding 120,000 HTG (approximately $3,000) or its equivalent in foreign currency. Many financial institutions, such as microfinance institutions, lotteries and insurance companies can be used as money laundering channels, since they are not regulated by any financial law. A draft banking law, before Parliament, will address this regulatory gap.

In 2002, Haiti formed a National Committee to Fight Money Laundering (CNLBA) under the supervision of the Ministry of Justice and Public Security. The CNLBA is in charge of promoting, coordinating, and recommending policies to prevent, detect, and suppress the laundering of assets obtained from the illicit trafficking of drugs and other serious offenses. Haiti's financial intelligence unit (FIU) established in 2003, the Unité Centrale de Renseignements Financiers (UCREF), falls under the supervision of the CNLBA. The UCREF's mandate is to receive and analyze reports submitted by financial institutions in accordance with the law. The UCREF has 34 employees, including five analysts. In 2008, reforms were undertaken to strengthen the institution. Institutions, including banks, credit unions, exchange brokers, insurance companies, lawyers, accountants, and casinos, are now required to report to the UCREF transactions involving funds that may be derived from a crime, as well as transactions that exceed 400,000 HTG (approximately $10,000) for which banks and currency exchangers must file a cash transaction report (CTR). Money transfer companies, given the high risk associated with them, have to file CTRs for all transactions amounting to at least 120,000 HTG (approximately $3,000). Failure to report such transactions is punishable by more than three years' imprisonment and a fine of 20 million HTG (approximately $550,000). Banks are required to maintain records for at least five years and to present this information to judicial authorities and UCREF officials upon request. Bank secrecy or professional secrecy cannot be invoked as grounds for refusing information requests from these authorities. Money launderers get around financial restrictions by

opening several bank accounts for less than 400,000 HTG per person (the threshold set by the AMLL) without rousing suspicion.

Although the government has publicly committed to combat corruption, the court system has been largely dysfunctional. None of the investigations initiated under the interim government have led to prosecutions. Implementation of the AMLL has been supported through the restructuring of UCREF, establishing it as a financial intelligence gathering body and through the reassignment of all criminal investigative responsibilities to the Bureau of Financial and Economic Affairs (BAFE), a component of the Haitian National Police (HNP) Office of Judicial Police (DCPJ), which has resulted in stalled cases moving forward. The BAFE includes, in addition to police officers (all of whom have received training in financial investigation techniques), two judges of instruction ("investigating magistrates") and two prosecutors. Trial judges with specialized financial knowledge have been identified to receive financial cases. The BAFE and UCREF have become engaged in providing evidence to support prosecutions in the United States. The UCREF and the BAFE are currently assisting the United States in at least three major investigations. The BAFE completed 44 financial investigations, of which eight have been submitted to the judicial authorities for prosecution.

The AMLL contains provisions for the seizure and forfeiture of assets; however, the government cannot seize and declare the assets forfeited until there is a conviction. The GOH has expanded the legal interpretation of conviction to include convictions obtained in foreign jurisdictions. In December 2008, the U.S. Securities Exchange Commission (SEC) halted the trading of an investment club run by a Haitian individual who targeted the Haitian community in South Florida and defrauded these investors of approximately $23.4 million. In the fourth quarter of 2008 the BAFE and UCREF, with U.S. Drug Enforcement Administration assistance, began seizing properties in Haiti belonging to drug traffickers incarcerated in the United States for use or disposal by the GOH. In 2008, 18 properties valued at over 21 million dollars, including residences, businesses and bank accounts, were seized and forfeited to the GOH based on U.S. convictions and another 20 properties are the subject of this new initiative.

Although the AMLL provides grounds for seizure it does not contain procedures to handle the management and proceeds of seized assets. The CONALD (National Drug Control Commission) is the agency responsible for managing seized and forfeited assets and is in the process of developing the infrastructure to maintain assets until they are disposed of following forfeiture. This change will empower the government to benefit from forfeited assets and their proceeds.

Flights to Panama City, Panama, remain the main identifiable mode of transportation for money couriers. Cash that is routinely transported to Haiti from Haitians and relatives in the United States in the form of remittances represented over 20 percent of Haiti's gross domestic product in 2007, according to the Central Bank. Remittances flows through official channels to Haiti were estimated at $1.18 billion in fiscal year 2007. 2008 statistics are not yet available. There is low confidence in the efforts of Haitian customs and narcotics personnel to interdict outbound funds concealed on the persons of travelers. Suspicions that clandestine fees are collected to facilitate the couriers continuing without arrest appear to be well-founded. Interdicted persons are frequently released by the courts and the funds are ordered to be returned. During interviews, couriers usually declare that they intend to use the large amounts of U.S. currency (between $30,000 and $100,000) to purchase clothing and other items to be sold upon their return to Haiti, a common practice in the informal economic sectors. Suspected drug flights from Venezuela and boat shipments from Jamaica continue to operate with impunity.

Corruption is an ongoing challenge to economic growth. Haiti is ranked one of the most corrupt countries in the world according to Transparency International's Corruption Perception Index for 2008. The GOH has made incremental progress in enforcing public accountability and transparency, but substantive institutional reforms are still needed. In 2004, the government established the

Specialized Unit to Combat Corruption (ULCC) in the Ministry of Economy and Finance. The ULCC is finalizing a draft bill for a national strategy to combat corruption, including requirements for asset declaration by public sector employees and a code of ethics for the civil service. ULCC will submit the national anticorruption law to Parliament for consideration in the coming months. A new Customs Code bill, which includes the designation of customs fraud as a money laundering offense, has been submitted to the Haitian Parliament.

Haiti has yet to pass legislation criminalizing the financing of terrorism, although counterterrorist financing legislation is being drafted with USG assistance. Haiti is not a party to the International Convention for the Suppression of the Financing of Terrorism. Haiti reportedly circulates the list of terrorists and terrorist organizations identified in UN Security Council Resolution 1267. The AMLL may provide sufficient grounds for freezing and seizing the assets of terrorists; however, given that there is currently no indication of the financing of terrorism in Haiti, this has not yet been tested. Haiti is a party to the 1988 UN Drug Convention, and has signed, but not ratified, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. Haiti is a member of the OAS/CICAD Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force (CFATF), a Financial Action Task Force (FATF)-style regional body. In September 2007, the World Bank conducted an assessment of the GOH that serves as a CFATF mutual evaluation. The UCREF is not a member of the Egmont Group of financial intelligence units but has memoranda of understanding (MOUs) with the FIUs of the Dominican Republic, Panama, Guatemala and Honduras.

Despite political instability, the Government of Haiti is making progress on addressing deficiencies in its anti-money laundering and counterterrorist financing regime through its efforts to improve its legal framework to combat drug trafficking, money laundering, and corruption, and its action to reform the judicial process. President Preval has made these improvements a key element of his national agenda. He is actively seeking technical assistance and cooperation with countries in the region to reinforce Haiti's institutional capacity to fight financial crime.

The Government of Haiti should finalize its draft legislation on terrorist financing to criminalize the financing of terrorism and become a party to the UN Convention for the Suppression of the Financing of Terrorism. Haiti should also ratify the UN Convention against Corruption and the UN Convention against Transnational Organized Crime. The GOH should move to enact the draft pieces of legislation pertaining to anticorruption and the new Customs Code bill. Haiti should further reinforce the capacity of the Haitian justice system to prosecute financial crimes; update the criminal code, reform the civil tax code and criminalize tax evasion as part of the country's anticorruption measures. Other areas in need of improvement include an ineffective court system, weak enforcement mechanisms and poor knowledge of current laws governing this area. The GOH should move quickly to prosecute cases of corruption, drug trafficking and money laundering. This could send a positive message that financial crimes will be punished to the fullest extent of the law and also help garner broader public support for the rule of law, as has occurred with the recent asset seizures. Finally, initiatives are needed to enhance the UCREF's capacity to provide timely and accurate reports on suspicious financial activities and meet the Egmont Group membership standards.

Honduras

Honduras is not an important regional or offshore financial center. Money laundering in Honduras stems primarily from significant narcotics trafficking, particularly cocaine, throughout the region. Human smuggling of illegal immigrants into the United States also constitutes a growing source of laundered funds. Laundered proceeds typically pass directly through the formal banking system, but remittance companies, currency exchange houses and automobile and real estate front companies may be increasing. High remittance inflows, which reached more than $2.6 billion, or 20 percent of gross domestic product in 2008, as well as smuggling of contraband goods, may also generate funds that are

laundered through the banking system. Honduras however, does not appear to be experiencing an increase in financial crimes such as bank fraud. Money laundering in Honduras derives both from domestic and foreign criminal activity, and the majority of proceeds are suspected to be controlled by local drug trafficking organizations and organized crime syndicates. Some illicit funds may also be laundered through the construction sector. The country's is vulnerable to the cross-border movement of contraband and illicit proceeds of crime as the citizens of Honduras, Guatemala, El Salvador, and Nicaragua, are permitted immigration inspection-free movement across their respective borders under the Central American Four Agreement, and there is no requirement for reporting border declarations and seizures to the financial intelligence unit. There is still a lack of adequate implementation and enforcement. These factors, combined with the vulnerabilities of a lack of resources for investigations and analysis, corruption within the law enforcement and judicial sectors, contribute to a favorable climate for significant money laundering in Honduras.

There is not a significant black market for smuggled goods, although there is some smuggling of items such as firearms, gasoline, illegally caught lobster and cigarettes. Though there are a growing number of free trade zones with special tax and customs benefits, there is no specific evidence Honduran free trade zone companies are being used in trade-based money-laundering schemes or by financiers of terrorism.

The Government of Honduras enacted its first money laundering legislation (Decree 202-97) enacted in December 1997. It came into force in early 1998 and criminalized the laundering of narcotics related proceeds. That legislation has evolved significantly since then. Law No. 27-98 criminalizes the laundering of narcotics-related proceeds and contains various record-keeping and reporting requirements for financial institutions. Decree No. 45-2002 supersedes the original money laundering laws established in 1998 by strengthening the legal framework and making available investigative and prosecutorial tools. The same decree expands the definition of money laundering to include transfer of assets that proceed directly or indirectly from trafficking of drugs, arms, human organs or persons; auto theft; kidnapping; bank and other forms of financial fraud; and terrorism, as well as any sale or movement of assets that lacks economic justification. The penalty for money laundering is 15 to 20 years. The decree also requires all persons entering or leaving Honduras to declare (and, if asked, present) cash and convertible securities that they are carrying if the amount exceeds $10,000 or its equivalent. As of 2008 a supplementary reporting form had not been implemented for individuals carrying more than $10,000, due to an unresolved disagreement between the two institutions over responsibility for record keeping. The discussion over the form revealed other weaknesses in cash smuggling enforcement. These include the lack of law enforcement authority for customs agents, and the fact that nondeclaration of more than $10,000 or the equivalent is not a distinct crime, although it is enough to make an individual a suspect. In 2008, ICE and Honduran Customs authorities conducted joint interdiction operations at Toncontin International Airport in Tegucigalpa, focusing on identifying individuals who failed to declare currency in excess of $10,000. The operations resulted in the seizure of over $55,000.

Decree No. 45-2002 also creates the financial intelligence unit (FIU), the Unidad de Información Financiera (UIF), within the National Banking and Insurance Commission (CNBS). Banks and financial institutions are required to report any suspicious transactions and all transactions over $10,000, or its equivalent to the UIF. According to the decree, reporting institutions must keep a registry of reported transactions for five years. Banks are required to know the identity of all their clients and depositors, regardless of the amount of deposits, and to keep adequate records. Banker negligence provisions subject individual bankers to two- to five-year prison terms if, by carelessness, negligence, inexperience, or nonobservance of the law, they permit money to be laundered through their institutions. Anti-money laundering requirements apply to all financial institutions that are regulated by the CNBS, including state and private banks, savings and loan associations, bonded warehouses, stock markets, currency exchange houses, securities dealers, insurance companies, credit

associations, and casinos. However, there is no implementation of AML requirements within the gaming industry.

Decree No. 129-2004 (Financial Systems Law) eliminates any legal ambiguity concerning the responsibility of banks to report information to the supervisory authorities, and the duty of these institutions to keep customer information confidential, by clarifying that the provision of information requested by regulatory, judicial, or other legal authorities shall not be regarded as an improper divulgence of confidential information. Under the Criminal Procedure Code, officials responsible for filing reports on behalf of obligated entities are protected by law with respect to their cooperation with law enforcement authorities. However, some bank executives have alleged that their personal security is put at risk if the information they report leads to the prosecution of money launderers.

Congress passed legislation in early 2008 that brings the Government of Honduras (GOH) closer to international legal standards for control of illicit financing, including money laundering and terrorist financing. Major amendments to the money laundering law clarify responsibilities for monitoring nonfinancial entities and a new chapter added to the penal code criminalizes terrorist financing. The amendments to the money laundering law gives the UIF oversight for collecting all suspicious transactions reports from banks, and expands the scope of entities required to report suspicious transactions to the UIF beyond the financial scope of the CNBS. Such entities include real estate agents, used car dealerships, antique and jewelry dealers, remittance companies, armed car contractors, and nongovernmental organizations. The reforms would also give the UIF sole oversight and responsibility not only for collecting suspicious transaction reports but also for analyzing and presenting to prosecutors cases deemed appropriate for prosecution.

The Public Ministry (Attorney General's Office and police all suffer from inadequate funding, limited capacity, and a lack of personnel and training.) Prosecutors expend the bulk of their limited resources focusing on high-profile crimes related to money laundering, such as narcotics trafficking, trafficking in persons, and cash smuggling. The UIF does not have direct access to law enforcement information in making its analyses, and does not have sufficient operational independence as prosecutors dictate to the UIF which cases to analyze based on suspicious transaction reports. The prosecutor charged with coordination with the UIF rarely visits his counterparts and is no longer working closely with the Office for Management of Seized Assets (OABI.) The number of convictions in 2008 was the lowest since 2003, the first full year that money laundering was a distinct crime in Honduras. In only two separate cases, seven individuals were found guilty of money laundering crimes, and one was absolved. Between 2003 and 2008, a total of 47 individuals were convicted in 32 separate cases. Only two of 54 ongoing investigations in 2007 originated from atypical financial reports.

Lack of coordination at all levels is a key area preventing a higher success rate in investigations and prosecutions. At the ministry level, the Interagency Commission for the Prevention of Money Laundering and Financing of Terrorism (CIPLAFT) was created in 2004 but never got off the ground. The current President of the CNBS does not believe he should be in charge of the CIPLAFT as specified by Presidential Decree, and as such has not convened any meetings. He told the U.S. Embassy in mid-2008 of his intention to propose another ministry take responsibility for the CIPLAFT, but has neither specified which ministry nor formally requested a change to his responsibilities. Although Decree 45-2002 requires that a public prosecutor be assigned to the UIF, the Special Prosecutor for Money Laundering personally acts as coordinator and contact is sporadic and personality-driven. Response times for information sharing between the UIF and the seized assets unit initially improved after a 2006 agreement between the Public Ministry, CNBS, and the UIF to prioritize money laundering cases. However, information sharing has stagnated in the last two years and has a backlog of about a year. In theory, the agreement should have streamlined the number of cases for potential prosecution and allowed many cases to be officially closed. The low number of convictions this year suggests otherwise. Adoption of the new anti-money laundering amendments should improve coordination and clarify division of responsibilities for investigations and reporting.

Remittance inflows, mostly from the United States, are growing slower this year due to global economic downturn, but still constitute about 20 percent of GDP and will likely top $2.6 billion in 2008. There has been no evidence to date linking these remittances to the financing of terrorism. The director of the UIF admits that remittances are extremely vulnerable to money laundering, but says Honduras lacks a formal tracking system to measure the extent of proceeds being laundered through formal and informal cross-border financial transfers. The remittance regulations in the new money laundering amendment now require remittance dealers not registered at the CNBS to report suspicious transactions. Once implementing regulations are put in place, the new amendment should give the UIF oversight capacity to properly investigate remittance companies. The CNBS securities superintendent has drafted the implementing regulations. The U.S. Internal Revenue Service (IRS) and Financial Crimes Enforcement Network (FinCEN), which serves as the U.S. financial intelligence unit, have provided comments and the implementing regulations should be activated within the first few months of 2009.

The GOH's asset seizure law has been in effect since 1993. The law allows for both civil and criminal forfeiture, and there are no significant legal loopholes that allow criminals to shield their assets. Decree No. 45-2002 strengthens the asset seizure provisions of the law, and establishes the OABI under the Public Ministry. Decree 45-2002 also authorizes the OABI to guard and administer all goods, products, or instruments of a crime and requires money seized or money realized from the auctioning of seized goods to be transferred to the public entities that participated in the investigation and prosecution of the crime.

The OABI is charged with distributing funds to various law enforcement units and nongovernmental organizations (NGOs). According to the Public Ministry, up to 50 percent of the proceeds gained by auctioning or selling seized goods go to the unit that performed the seizure. An additional 25 percent of the proceeds go to institutions involved in crime prevention and rehabilitation of criminals and the balance goes to OABI's support budget. In reality, equitable sharing of seized monies has been a continuing problem, and appears at times to be controlled by political influence. Police entities involved in the original investigations rarely see an equitable share of the assets seized and investigators often must ride public buses to conduct investigations. In some cases, entities that have nothing to do with the investigation receive an unjustified portion of the funds.

The OABI is a poorly administered organization, and is constrained by a lack of coordination with public prosecutors who must bring cases to trial before seized assets can be distributed or auctioned. The public prosecutor has said it is no longer working with OABI because of disputes over final forfeiture of assets and disbursement of monies from auctioned assets or bulk cash seizures. Momentum is now gaining for OABI to more quickly liquidate all assets once confiscated, in an effort to avoid parking lots full of deteriorating assets and high protection and maintenance fees. With new management and guidelines in place, and the new witness protection law that passed in 2008 which allows the unit to hold all seized assets, OABI could expand its role significantly. Police and prosecutors complain the witness protection law cannot be enforced without the necessary funding.

Decree No. 45-2002 leaves ambiguous the question of whether legitimate businesses found to be laundering money derived from criminal activities can be seized. Although the chief prosecutor for organized crime believes that businesses laundering criminal assets cease to be "legitimate," subjecting them to seizure and prosecution, this authority is not explicitly granted in the law. There has been no test case to date that would set an interpretation. There are currently no new laws being considered regarding seizure or forfeiture of assets of criminal activity. Equally ambiguous is the ability of the prosecutor's office to seize individual or business assets based on "unexplained enrichment." Though a recent World Bank report on Honduran compliance with international standards criticized the practice and pointed out that no such legislation exists elsewhere, the prosecutor's office insists it must act on ambiguous information at times.

Under the Criminal Procedure Code, when goods or monies are seized in any criminal investigation, a criminal charge must be submitted against the suspect within 60 days of the seizure; if one is not submitted, the suspect has the right to demand the release of the seized assets. This places financial pressure on OABI, which is responsible for maintaining assets at high expense while prosecutors investigate and build cases.

As of December 2008, the total value of assets seized since Decree 45-2002 came into effect was approximately $5.9 million, including $4.6 million in tangible assets such as cars, houses, and boats. The total for 2008 barely increased in comparison to 2007 because there has been little to no movement in existing cases and few seizures this year. $750,000 collected from the sale of an abandoned plane in 2007, probably related to narcotics, was used to purchase several cars for public prosecutors and police investigators. Most of these seized assets have derived from crimes related to drug trafficking; none is suspected of being connected to terrorist activity.

Decree 45-2002 was amended in April 2008, and now designates both terrorist financing and asset transfer related to terrorism as crimes. This is a major step to bring Honduras into accordance with the Financial Action Task Force (FATF) Forty-Nine recommendations. The crime of terrorist financing now carries a 20 to 30 year prison sentence, along with a fine of up to $265,000.

Under separate authority, the Ministry of Foreign Affairs is responsible for instructing the CNBS to issue freeze orders for organizations and individuals named by the United Nations Security Council Resolution (UNSCR) 1267 and those organizations and individuals on the list of Specially Designated Global Terrorists by the United States pursuant to Executive Order 13224. The Commission directs Honduran financial institutions to search for, hold, and report on terrorist-linked accounts and transactions, which, if found, would be frozen. Both the Ministry of Foreign Affairs and CNBS have responded promptly to these requests. CNBS has reported that, to date, no accounts linked to the entities or individuals on the lists have been found in the Honduran financial system.

Honduras cooperates with United States investigations and requests for information pursuant to the 1988 United Nations Drug Convention. No specific written agreement exists between the U.S. and Honduras to establish a mechanism for exchanging adequate records in connection with investigations and proceedings relating to narcotics, terrorism, terrorist financing, and other crime investigations. However, Honduras has cooperated, when requested, with appropriate law enforcement agencies of the U.S. Government and other governments investigating financial crimes. The UIF has signed memoranda of understanding to exchange information on money laundering investigations with Panama, El Salvador, Guatemala, Mexico, Peru, Colombia, the Dominican Republic, Costa Rica, Bolivia, Haiti, Argentina, Saint Vincent and The Grenadines, St. Kitts and Nevis, Belize, and the Cayman Islands. The UIF has reported that bilateral cooperation and information sharing is good across the board.

Honduras is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. At the regional level, Honduras is a member of the Central American Council of Bank Superintendents, which meets periodically to exchange information. Honduras is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Group of Experts to Control Money Laundering, and the Caribbean Financial Action Task Force (CFATF), a FATF-style regional body. In 2005, the UIF became a member of the Egmont Group.

The World Bank Financial Sector Assessment Program (FSAP) completed an assessment of Honduran compliance with international money laundering standards in February 2008. The report describes and analyzes anti-money laundering and counterterrorist financing measures, sets out Honduras' levels of compliance with the FATF Forty-Nine Recommendations. The draft report recognizes that Honduras is close to compliance with a large number of international legislation and norms, but criticizes lack of

implementation and enforcement, and a "systematic lack of coordination" between key players. In addition, the report noted that GOH does not require sufficient transparency with regard to the beneficial ownership of legal persons. The UIF will respond to the report on behalf of the Government of Honduras at the CFATF, Plenary meeting in Trinidad and Tobago in May 2009.

The Government of Honduras (GOH) made progress in 2008 by criminalizing terrorist financing and increasing the legal scope of financial entities to be monitored by the UIF. The GOH should ensure that these improvements to money laundering regulations are implemented, enforced, and coordinated in order to bring its anti-money laundering and counterterrorist financing regime into greater compliance with international standards. In the interim, the GOH should continue to support the developing law enforcement and regulatory entities responsible for combating money laundering and other financial crimes. The GOH should also resolve any ambiguity regarding the seizure of businesses used for criminal purposes and suspicious enrichment of individuals, and should repeal provisions which allow for a waiver of criminal liability for first time legal person offenders. The Government of Honduras should pay special attention to the need for stronger coordination between entities which is the single largest factor inhibiting the fight against money laundering.

Hong Kong

Hong Kong is a major international financial center. Its low taxes and simplified tax system, sophisticated banking system, shell company formation agents, and the absence of currency and exchange controls facilitate financial activity but also make Hong Kong vulnerable to money laundering. The Hong Kong Special Administrative Region Government (HKSARG) considers the primary sources of laundered funds to be corruption (both foreign and domestic), tax evasion, fraud, illegal gambling and bookmaking, prostitution, loan sharking, commercial crimes, and intellectual property rights infringement. Laundering channels include Hong Kong's banking system, legitimate and underground remittance and money transfer networks, trade-based money laundering, and large-ticket consumer purchases—such as property, gold and jewelry. The proceeds from narcotics trafficking are believed to be only a small percentage of illicit proceeds laundered.

Hong Kong is a free port. As such, there is no significant black market for smuggled goods. According to Hong Kong law enforcement authorities, there is no evidence to suggest smuggling activities in Hong Kong are funded by narcotics proceeds.

Hong Kong has investigated and prosecuted very few money laundering cases involving fund movements outside the formal banking sector. The formal banking sector appears to be the primary means by which criminals attempt to launder funds in Hong Kong. Over the past four years, reported financial crimes have increased. Hong Kong police reported 4,758 (2006) and 4,745 (2007) cases of Deception; Business Fraud cases totaled 34 (2006) and 27 (2007); Forgery and Coinage cases reported totaled 1,149 (2006) and 1,195 (2007). Hong Kong does not keep separate statistics on cases involving U.S. currency. The government expects the current economic downturn to lead to increased financial crime and is tightening its supervision of the banking system.

Hong Kong does not make a distinction between onshore and offshore entities, including banks. Its financial regulatory regimes are applicable to residents and nonresidents alike. No differential treatment is provided for nonresidents, including with respect to taxation and exchange controls. The Hong Kong Monetary Authority (HKMA) regulates banks. The Office of Commissioner of Insurance (OCI) and the Securities and Futures Commission (SFC) regulate insurance and securities firms, respectively. All three impose licensing requirements and screen business applicants. There are no legal casinos or Internet gambling sites in Hong Kong.

In Hong Kong, it is not uncommon to use solicitors and accountants, acting as company formation agents, to set up shell or nominee entities to conceal ownership of accounts and assets. Many of the

more than 500,000 international business companies (IBCs) registered in Hong Kong are established with nominee directors; and many are owned by other IBCs registered in the British Virgin Islands. However, all companies are required to file certain information on an annual basis with the Companies Registry, including annual accounts, details of registered offices, directors, the company secretary, charges, a register of members and debenture holders (depending on the category of companies to which a company belongs). In addition, these companies are subject to additional regulatory controls if they engage in certain business activities. For example, if a company carries out banking/securities/insurance business, it must conduct customer due diligence on all corporate entities and trust arrangements, in particular, identifying their beneficial owners for the purpose of complying with the AML/CTF requirements of the HKMA, SFC, and/or OCI. The AML/CTF guidelines published by these three regulators require companies to have procedures in place to monitor the identity of all principal shareholders, directors, account signatories and the beneficial owner of the corporate customer. Bearer shares are not permitted for companies registered in Hong Kong.

Money laundering is a criminal offense in Hong Kong under the Drug Trafficking (Recovery of Proceeds) Ordinance (DTRoP) and the Organized and Serious Crimes Ordinance (OSCO). The two ordinances provide for the tracing, restraint and confiscation of proceeds derived from drug trafficking and other serious crimes. The legislation also criminalizes the act of dealing with property while knowing or having reasonable grounds to believe that such property represents proceeds of drug trafficking and other indictable offenses. The money laundering offense extends to the proceeds of drug-related and other indictable crimes. Money laundering is punishable by up to 14 years' imprisonment and a fine of HK $5,000,000 (approximately U.S. $641,000). Hong Kong enacted the United Nations (Anti-Terrorism Measures) Ordinance (UNATMO) (Cap. 575) in 2002 to criminalize terrorism and terrorist financing. UNATMO was amended in 2004 to allow Hong Kong to freeze the nonfund property of terrorists and terrorist organizations.

Money laundering ordinances apply to covered institutions—including banks and nonbank financial institutions—as well as to intermediaries such as lawyers and accountants. All persons must report suspicious transactions of any amount to the Joint Financial Intelligence Unit (JFIU). There is no minimum threshold that compels reporting. The JFIU does not investigate suspicious transactions itself but receives, stores, and disseminates suspicious transactions reports (STRs) to the appropriate investigative unit. Typically, STRs are passed to the Narcotics Bureau, the Organized Crime and Triad Bureau of the Hong Kong Police Force, or to the Customs Drug Investigation Bureau of the Hong Kong Customs and Excise Department. No laws in Hong Kong contain secrecy provisions that prohibit authorized institutions from disclosing client and ownership information to the HKMA and the law enforcement agencies.

Financial regulatory authorities have issued anti-money laundering guidelines reflecting the revised FATF Forty Recommendations on Money Laundering to institutions under their purview and monitor compliance through on-site inspections and other means. The HKMA is responsible for supervising and examining compliance of financial institutions that are authorized under Hong Kong's Banking Ordinance. The SFC is responsible for supervising and examining compliance of persons that are licensed by the SFC to conduct business in regulated activities, as defined in Schedule 5 of the Securities and Futures Ordinance. The OCI is responsible for supervising and examining compliance of insurance institutions. Hong Kong law enforcement agencies provide training and feedback on suspicious transaction reporting.

Financial institutions are required to know and record the identities of their customers and maintain records for five to seven years. The filing of a suspicious transaction report cannot be considered a breach of any restrictions on the disclosure of information imposed by contract or law. Remittance agents and moneychangers must register their businesses with the police and keep customer identification and transaction records for cash transactions above a legal threshold for at least six

years. An HKMA directive reduced this threshold amount from HK $20,000 (approximately U.S. $2,565) to HK $8,000 (approximately U.S. $1,000), effective January 1, 2007.

Hong Kong does not require reporting of the movement of any amount of currency across its borders, or of large currency transactions above any threshold level. Hong Kong is examining the effectiveness of its existing regime in interdicting illicit cross border cash couriering activities. Reportedly, Hong Kong is deliberating ways of complying with FATF Special Recommendation Nine but does not intend to put in place a "declaration system" and is instead considering a disclosure-based system. Law enforcement agents in Hong Kong are already empowered to seize criminal proceeds anywhere in the jurisdiction, including at the border.

Designated Non-Financial Businesses and Professions as defined by FATF (i.e. lawyers, accountants, estate agents, trust and company service providers and dealers in precious stones and metals) are not subject to specific statutory AML/CTF requirements. However, under the DTROP, the OSCO and the UNATMO, suspicious transaction reporting requirements are applicable to all persons. Lawyers, accountants, practitioners in nonfinancial institutions, dealers in precious stones and precious metals are all obliged by law, as are all persons, to make a suspicious transaction report to the JFIU if they come across any property known or suspected to be proceeds of drug trafficking, crimes, or terrorism. Under the DTROP, the OSCO and the UNATMO, all persons are required to report his/her knowledge or suspicion of crime proceeds or terrorist property; failure to report such suspicion or knowledge is a criminal offense. The reporting requirement exists irrespective of the value of the proceeds or property, and the circumstances by which the person comes across such knowledge or suspicion.

In addition, the professional bodies or regulators of Hong Kong lawyers, accountants, estate agents, trust and company service providers have issued AML/CTF guidelines and encourage their members to comply. During 2008, the Narcotics Division of the Hong Kong Security Bureau and the JFIU have conducted regular outreach and capacity building programs for these sectors including seminars, guidelines, leaflets and Announcements in the Public Interest on television and radio.

Hong Kong's open financial system has long made it the primary conduit for funds transferred out of China. Hong Kong's role has been evolving as China's financial system gradually opens. On February 25, 2004, Hong Kong banks began to offer Chinese currency-based (renminbi or RMB) deposit, exchange, and remittance services. Later that year, Hong Kong banks began to issue RMB-based credit cards, which could be used both in Mainland China and in Hong Kong shops that had enrolled in the Chinese payments system, China Union Pay. In November 2005, Hong Kong banks were permitted modest increases in the scope of RMB business they can offer clients. The new provisions raised daily limits to 20,000 RMB (approximately $3000) and expanded services. This change brought many financial transactions related to China out of the money-transfer industry and into the more highly regulated banking industry, which is better equipped to guard against money laundering.

Despite Hong Kong's efforts to encourage capital shifts to the banking industry, Chinese capital controls continue to encourage entities in both Hong Kong and Mainland China to use underground financial systems to avoid Chinese restrictions on currency exchange. A well-publicized June 2007 raid by Chinese police on an underground bank in Shenzhen resulted in the detention of six suspects, including a Hong Kong-based businesswoman, accused of facilitating the transfer of RMB 4.3 billion (approximately. $570 million) out of China since the beginning of 2006—including transfers by Chinese state-owned enterprises. Authorities believe the majority of these funds were used to purchase properties and stocks in Hong Kong. Media reports indicated that such underground exchange houses are rampant in Guangdong province and have transferred more than RMB 200 billion (U.S. $26.7 billion) out of China since 2006. While Chinese police action in late 2007 appears to have dealt a blow to underground banking systems, the lack of strong Hong Kong government oversight of moneychangers and remittance agents was highlighted in the FATF/APG Mutual Evaluation Report, published in June 2008. The global economic slowdown and a dramatic drop in Hong Kong housing

and equity prices are likely to have contributed as much to declining crossborder flows as to stricter enforcement on the part of the Chinese and Hong Kong authorities.

To facilitate effective processing of suspicious transaction reports, the Joint Financial Investigation Unit (JFIU), staffed by the HKP and Customs and Excise Department, has been in operation since 1989. It collects and processes suspicious transaction reports, analyzes the information contained therein, and disseminates the reports to the appropriate law enforcement units for further investigation. The JFIU also conducts research on money laundering trends and methods and provides case examples (typologies) to financial and nonfinancial institutions to assist them in identifying suspicious transactions. The JFIU has no regulatory responsibilities.

The Hong Kong JFIU is housed in a separate, secure area in the Narcotics Bureau within the Police Headquarters Complex. It is treated as a separate unit and acts independently from other police units in order to preserve its autonomy and independence. While the JFIU is considered a separate and distinct unit, it does not have any independent or devolved budget. Day-to-day operating costs are met from the budgets of the Police and Customs and Excise Departments. JFIU receives disclosures, conducts analysis on them, and in suitable cases distributes them to investigation units. JFIU can distribute cases to all Hong Kong law enforcement agencies, similar overseas bodies and in certain circumstances regulatory bodies in Hong Kong.

The JFIU has direct access to the records and databases maintained within the Police and Customs and Excise Departments. It also has direct access to the databases of the Transport Department, the Companies Registry and the Land Registry. Access to records maintained by other government agencies can be granted upon JFIU's written request and in the case of the tax authority, a court order. Financial institutions are obligated to provide the JFIU with any information relating to a suspicious transaction that it has reported. However, the JFIU does not have access to the databases of financial institutions. If more detailed information is required in respect of suspicious transaction reports, the financial institution must be formally subpoenaed. Section 12(6) of the UNATMO and Sections 25A (9) of both the DTROP and the OSCO allow for the dissemination of information to domestic and foreign agencies to combat crime and terrorism. Hong Kong legislation does not require JFIU to enter into MOUs with overseas counterparts for the purpose of information exchange. Up to the end of October 2008, the JFIU had received 12,560 STRs in 2008, of which 2,101 had been referred to law enforcement agencies for further investigation. Since 1994, when OSCO first mandated the filing of suspicious transaction reports (STRs), the number of STRs received by JFIU has generally increased. In the first nine months of 2007, 12,308 STRs were filed, of which 1798 were referred to law enforcement agencies.

The Hong Kong Police have a number of dedicated units responsible for investigating financial crime. The Commercial Crime Bureau and Narcotics Bureau are the primary units responsible for investigating money laundering and terrorist financing cases. Serious Crimes Squads in Police Districts are responsible for investigating less serious financial crimes. Resources and training are adequate for their current mission. The Independent Commission Against Commission (ICAC) investigates money laundering cases related to corruption while the Financial Investigation Group (FIG) of the Customs and Excise Department is responsible for money laundering investigations related to drug trafficking and organized crime.

As of the end of September 2008, Hong Kong law enforcement agencies had prosecuted 267 persons for financial crimes. However, the HKP has not reported any financially significant cases during 2008. Hong Kong Customs and Excise reported two arrests and one prosecution for money laundering since January 1, 2008.

Under the DTRoP and the OSCO, a court may issue a restraining order against a defendant's property at or near the time criminal proceedings are instituted. Property includes money, goods, real property, and instruments of crime. A court may issue confiscation orders at the value of a defendant's proceeds

from illicit activities. Cash imported into or exported from Hong Kong that is connected to narcotics trafficking may be seized, and a court may order its forfeiture. Legitimate businesses can be seized if the business is the "realizable property" of a defendant. Realizable property is defined under the DTRoP and OSCO as any property held by the defendant, any property held by a person to whom the defendant has directly or indirectly made a gift, or any property that is subject to the effective control of the defendant. The Secretary of Justice is responsible for the legal procedures involved in restraining and confiscating assets. There is no time frame ascribed to freezing drug proceeds or the proceeds of other crimes. Regarding terrorist property, a formal application for forfeiture must be made within two years of freezing. Confiscated or forfeited assets and proceeds are paid into general government revenue.

In July 2002, the legislature passed several amendments to the DTRoP and OSCO to strengthen restraint and confiscation provisions. These changes, effective January 1, 2003, lowered the evidentiary threshold for initiating confiscation and restraint orders against persons or properties suspected of drug trafficking, eliminated the requirement of actual notice to an absconded offender, eliminated the requirement that the court fix a period of time in which a defendant is required to pay a confiscation judgment, authorized courts to issue restraining orders against assets upon arrest rather than charging, required the holder of property to produce documents and otherwise assist the government in assessing the value of the property, and created an assumption under the DTRoP (to make it consistent with OSCO) that property held within six years of the violation by a person convicted of drug money laundering constitutes proceeds from that money laundering.

Hong Kong normally confiscates crime proceeds only after conviction in a court of law. However, the court may allow property seized on being imported into Hong Kong to be forfeited, if it is satisfied that such property is related to drug trafficking. The court may, on an application by the Secretary for Justice, order the forfeiture of terrorist property. An order may be made under either of these provisions independent of any criminal proceedings with which the property concerned is connected. The civil standard of proof applies in these proceedings. There are provisions under DTROP and OSCO to trace, seize and freeze assets without undue delay. The system for freezing and forfeiture of terrorist property is provided for under the UNATMO.

The year-end running balance for assets frozen and seized and the accumulative amounts of assets forfeited with reference to narcotics-related (DTROP) and criminal-related (OSCO) offenses for the past five years are provided below. There is a progressive increase in the confiscation for criminal-related offenses, reflecting additional efforts made by Hong Kong law enforcement agencies. No terrorist-related assets have been frozen, seized, and/or forfeited. Banks and other financial institutions cooperate with law enforcement efforts to seize or freeze bank accounts. According to JFIU figures as of September 30, 2008, the value of assets under restraint (pending confiscation proceedings) was $306.42 million, and the value of assets under a court confiscation order but not yet paid to the government was $10.07 million. JFIU also reported that, as of September 30, 2008, $58.44 million had been confiscated and paid to the government since the enactment of DTRoP and OSCO. The value of assets under restraint (pending confiscation proceedings) for 2007 was $265.44 million. The value of assets under a court confiscation order but not yet paid to the government was $10.96 million in 2007. The value of assets confiscated and paid to the government in 2007 was $56.18 million. No figures were available for 2008. Hong Kong has shared confiscated assets with the United States.

On July 3, 2004, the Legislative Council passed the United Nations (Anti-Terrorism Measures) (Amendment) Ordinance. This law is intended to implement UNSCR 1373 and the FATF Special Eight Recommendations on Terrorist Financing in place in July 2004. It extends the HKSARG's freezing power beyond funds to the property of terrorists and terrorist organizations. It also criminalizes the provision or collection of funds by a person intending or knowing that the funds will be used in whole or in part to commit terrorist acts. Hong Kong's financial regulatory authorities have directed the institutions they supervise to conduct record searches for assets of suspected terrorists and

terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. There has been no legislation to comport with special Recommendation Nine on cash couriers.

To help deal with anti-money laundering (AML) issues from a practical perspective and reflect business needs, the Hong Kong Monetary Authority (HKMA) established an Industry Working Group on AML. Three subgroups have been established to share experiences and consider the way forward on issues such as politically exposed persons (PEPs), terrorist financing, transaction monitoring systems and private banking issues. The subgroup on Customer Due Diligence (CDD) issued guidelines on issues related to PEPs in November 2007. The HKMA has also implemented a number of initiatives on AML issues, including issuing circulars and guidance to authorized institutions on combating the financing of weapons of mass destruction conducting in-depth examinations of institutions' AML controls and setting out best practices for AML in high-risk areas—such as correspondent banking, private banking, and remittance. However, Hong Kong's 2008 FATF/APG Mutual Evaluation pointed to lack of sufficient oversight of informal financial entities, including remittance agents and money changers. Hong Kong authorities are expected to submit a proposal in early 2009 to increase supervision of these entities.

The HKMA circulated guidelines that require banks to maintain a database of terrorist names and management information systems to detect unusual patterns of activity in customer accounts. The SFC and the OCI circulated guidance notes in 2005 that provided additional guidance on CDD and other issues, reflecting the new requirements in the Revised FATF Forty Recommendations on Money Laundering and Special Recommendations on Terrorist Financing. In 2006, the OCI and the SFC revised their guidance notes to take into account the latest recommendations by the FATF. There are no special provisions in Hong Kong law to monitor the financial activities of charitable or nonprofit agencies.

Other bodies governing segments of the financial sector are also engaged in advancing anti-money laundering efforts. The Hong Kong Estates Agents Authority, for instance, has drawn up specific guidelines for real estate agents on filing suspicious transaction reports; and the Law Society of Hong Kong and the Hong Kong Institute of Certified Public Accountants are in the process of drafting such guidance for their members.

Hong Kong is an active member of the Financial Action Task Force's FATF and Offshore Group of Banking Supervisors and was a founding member of the Asia Pacific Group on Money Laundering (APG).

In November 2007, the APG and FATF conducted a site visit as part of their joint mutual evaluation of Hong Kong. The report, which was discussed at FATF's June 2008 Plenary meeting, praised Hong Kong's AML and CTR regime but identified a lack of oversight for remittance agents and money changers, and the designated nonfinancial business and professions such as accountants and lawyers, the lack of statutory backing for customer due diligence and record keeping requirements for financial institutions, and gaps in Hong Kong's legal framework to fully implement the United Nations Terrorist Financing Convention. Hong Kong is required to submit a report on its progress toward addressing these deficiencies in June 2010. Hong Kong plans to conduct a comprehensive review of its legal and regulatory regime and introduce specific measures to improve its ability to prevent, detect, investigate, enforce and prosecute money laundering and terrorist financing activities. The initial phase of the review will focus on the AML/CTF regulatory regime for the financial services sectors. Consultation with the concerned sectors is expected to follow publication of concrete proposals early in 2009. To ensure that the AML/CTF measures do not conflict with policies to promote Hong Kong as an international financial centre, the Financial Services and the Treasury Bureau has taken over from the Security Bureau the overall coordinating role for AML/CTF policies within the Administration, beginning in October 2008.

The People's Republic of China (PRC) represents Hong Kong on defense and foreign policy matters, including UN affairs. Through the PRC, the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the UN International Convention for the Suppression of the Financing of Terrorism are all applicable to Hong Kong.

Hong Kong's banking supervisory framework is in line with the requirements of the Basel Committee on Banking Supervision's "Core Principles for Effective Banking Supervision." Hong Kong's JFIU is a member of the Egmont Group and is able to share information with its international counterparts. Hong Kong is known to cooperate with foreign jurisdictions in combating money laundering.

Hong Kong's mutual legal assistance agreements generally provide for asset tracing, seizure, and sharing. Hong Kong signed and ratified a mutual legal assistance agreement (MLAA) with the United States that came into force in January 2000. Hong Kong has MLAAs with 25 other jurisdictions. Hong Kong has also signed surrender-of-fugitive-offenders (extradition) agreements with 17 countries, including the United States, and has signed agreements for the transfer of sentenced persons with ten countries, also including the United States. Hong Kong authorities exchange information on an informal basis with overseas counterparts and with Interpol. Apart from exchange of intelligence and other information permissible at the law enforcement level, documentary evidence may also be provided pursuant to money laundering and terrorist financing investigations or proceedings pursuant to requests made under the operative agreement with the United States on mutual legal assistance. Hong Kong provides similar assistance to jurisdictions that have operative bilateral or multilateral agreements with United States or on the basis of reciprocity under the MLAA.

In 2008, Hong Kong Customs conducted two successful joint operations with the U.S. Drug Enforcement Agency (USDEA) and U.S. Immigration and Customs Enforcement (USICE). For the joint operation with DEA, crime proceeds of approximately HKD 8 million held by the key member of a drug-related money-laundering syndicate was restrained under the MLAA in Hong Kong in August 2008. The arrested person was eventually extradited to the United States in October 2008. For the joint operation with USICE, a subject from Taiwan was successfully extradited to the United State in August 2008. ICAC has responded to a Letter of Request regarding a corruption case involving a principal official of the Macau SAR for the production of bank records.

The Government of Hong Kong should further strengthen its anti-money laundering/counterterrorist financing regime by requiring more stringent customer due diligence and record keeping requirements for financial institutions; mandating more suspicious transaction reporting by lawyers and accountants, as well as by business establishments, such as auto dealerships, real estate companies, and jewelry stores ;establishing threshold reporting requirements for currency transactions; and putting into place "structuring" provisions to counterevasion efforts. . Hong Kong should institute mandatory oversight for remittance agents and money changers, and the designated nonfinancial business and professions such as accountants and lawyers. It should also establish mandatory cross-border currency reporting requirements and address trade-based money laundering, as well as monitor the financial activities of charitable or nonprofit agencies. . Hong Kong should also take steps to stop the use of "shell" companies, IBCs, and other mechanisms that conceal the beneficial ownership of accounts by more closely regulating corporate formation agents.

.

Hungary

Because of Hungary's advantageous and pivotal location in central Europe, a cash-based economy, and a well-developed financial services industry, money laundering in Hungary is related to a variety of criminal activities, including illicit narcotics-trafficking, prostitution, trafficking in persons, and organized crime. Criminal organizations (especially those from Russia and Ukraine) have become

well-established in Hungary. Several factors contribute to the prevalence of organized crime in Hungary. First, Hungary shares borders with seven other countries and is within the borders of the European Union (EU), thereby making it one of the largest markets for organized criminal activity. Second, as a transshipment country, Hungary's most vulnerable borders are the non-EU eastern and southern ones, such as those with Ukraine (cigarette and human trafficking) and Serbia (drug and arms trafficking), as well as Romania (human trafficking and prostitution). Finally, compared to other countries in the region, Hungary has a well-developed transportation system, facilitating the operation of criminal enterprises. Other prevalent economic and financial crimes include official corruption, tax evasion, real estate fraud, and identity theft (copying/theft of bankcards). Money laundering reportedly has not increased in recent years though there have been some isolated, albeit well-publicized, cases.

The Government of Hungary (GOH) has worked continuously to improve its anti-money laundering/counterterrorist financing (AML/CTF) enforcement regime and to implement the Financial Action Task Force (FATF) Forty Recommendations and the Nine Special Recommendations on Terrorist Financing.

A provision on the money laundering offense [Section 303 of the Hungarian Criminal Code (HCC) as amended by Act XXVII of 2007 (Act XXVII)] enlarges the scope of the money laundering offense to cover the transfer of proceeds to a third party even if it is carried out through a nonbanking or nonfinancial transaction. Act XXVII also addresses problems that have occurred within the AML reporting regime. Strict criminal penalties for nonreporting have resulted in over-filing by Hungarian financial institutions. This, in turn, has resulted in a high volume of suspicious transaction report (STRs) that are reportedly of low quality. Act XXVII reduces the maximum punishment for intentional noncompliance with reporting obligations from three years imprisonment to two years imprisonment. Hungary has also abolished the negligent form of nonreporting as a criminal offence.

The Government of Hungary (GOH) bans offshore financial centers, including casinos, by Act CXII of 1996 on Credit Institutions (Act CXII). Hungary discontinued its preferential tax treatment for offshore centers at the end of 2005; and in 2006 these companies automatically became Hungarian companies. The only special status they retain is the ability to keep financial records in foreign currencies. Hungary no longer permits the operation of free trade zones.

Act CXII bans the use of any indigenous alternative remittance systems that bypass, in whole or in part, financial institutions. The GOH has prohibited the use of anonymous savings booklets since 2001. Act CXX of 2001 eliminates bearer shares and requires that all such shares be transferred to identifiable shares. All shares now are subject to transparency requirements and all owners and beneficiaries must be registered. By mid-2003, Hungary had successfully transferred 90 percent of anonymous savings accounts into identifiable accounts. Individuals with remaining anonymous passbook accounts now need written permission from the police to access their accounts. The total balance remaining in anonymous accounts is approximately 12 billion HUF (approximately $60,200,000) for 2.82 million owners, corresponding to an average account size of 4,250 HUF (approximately $21). This total is mainly comprised of accounts for which savings booklets were lost, accounts whose holders have not proceeded with the conversion nor tried to make a withdrawal, and accounts whose original owners have died and their heirs do not know how to access the funds.

Hungary re-codified its original anti-money laundering (AML) legislation, Act XV of 2003 on the Prevention and Impeding of Money Laundering. The implementing regulations entered into force in August 2006. These measures ensure uniform implementation with regard to the definition of "politically exposed persons" (PEPs), the technical criteria for simplified customer due diligence (CDD) procedures, and exemptions for financial activity conducted on an occasional or very limited basis.

On November 19, 2007, the Parliament adopted Act CXXXVI on the Prevention and Combating of Money Laundering and Terrorist Financing (AML/CTF Act). The AML/CTF Act was published on

November 28, 2007, and entered into force on December 15, 2007. The AML/CTF Act establishes the legislative framework for preventing and combating terrorist financing and complies with international AML standards and requirements. The AML/CTF Act expands the scope of covered entities to cover the following professions: financial services, investment services, the insurance industry, commodity exchange services, postal money orders and transfers, real estate agents, auditors, accountants, tax advisors, casinos, jewelry merchants, lawyers, and notaries. The AML/CTF Act introduces more specific and detailed provisions relating to customer and beneficial owner identification and verification. The act introduces a risk-sensitive approach regarding CDD and establishes detailed rules, including simplified as well as enhanced CDD for low- or high-risk customers or business relationships, and appropriate procedures to determine whether a person is a PEP. The AML/CTF Act also addresses originator information accompanying transfers of funds. The Act contains provisions on internal training and communication procedures, detailing special protocols for lawyers and notaries. Safe harbor provisions protect individuals executing their AML/CTF reporting obligations.

Obliged entities must send a STR to the financial intelligence unit (FIU) and suspend the transaction if there is suspicion of money laundering or terrorist financing. The AML/CTF Act sets out the requirements for disclosure of information, and mandates the keeping of statistics so the effectiveness of the AML/CTF measures can be evaluated.

Only banks or their authorized agents can operate currency exchange booths, of which there are approximately 300 in Hungary. These exchange houses are subject to the banks' internal control mechanisms as well as to supervision by the Hungarian Financial Supervisory Authority (HFSA). The AML/CTF Act contains threshold-reporting requirements for currency exchange enterprises. Exchange booths must verify customer identity for currency exchange transactions totaling or exceeding 500,000 HUF (approximately $2,500), whether in a single transaction or derived from consecutive separate transactions. Exchange booths must file STRs for suspicious transactions in any amount.

Act No. XLVIII of 2007 states the Hungarian customs authorities should record the declarations of travelers entering or leaving the European Community with cash totaling or exceeding 10,000 euros (approximately $13,500) as well as the data collected in connection with any inspection of the declaration. If the data suggests money laundering or terrorist financing, the Hungarian Customs and Finance Guard (HCFG) must immediately send an STR to the FIU.

Hungary's financial regulatory body, the HFSA, supervises financial service providers with the exception of cash processors, which are supervised by the National Bank of Hungary. The Hungarian Tax and Financial Control Administration supervises casinos. The FIU supervises most designated nonfinancial businesses and professions (DNFBPs), such as real estate agents, accountants and tax advisors. In certain cases, DNFBP supervisory functions are performed by self-regulatory bodies: the Hungarian Bar Association with respect to lawyers, the Hungarian Association of Notaries Public with respect to notaries public, and the Chamber of Hungarian Auditors and Auditing Activities with respect to auditors. The Hungarian Trade Licensing Office is the supervisory authority with respect to natural and legal persons trading in goods and allowing cash payments above the amount of 3.6 million forints (approximately $18,000).

In 2006, the HFSA established a new division to deal with money laundering and financial crimes. The division coordinates supervisory tasks related to money laundering and terrorist financing and also assists other departments of the HFSA with on-site inspections. In 2007, the HFSA enlarged the staff of its Financial Forensic division. The HFSA established a standing AML/CTF working group that includes representatives of financial institutions and their associations.

Hungary's FIU, the Central Criminal Investigation Bureau (CCIB) was originally established in 1995 as a unit under the Hungarian National Police (HNP) where it was named the National Bureau of Investigation's Anti-Money Laundering Department (ORFK). A January 2008 amendment to Act XIX

of 1998 on the Hungarian Criminal Procedure transfers the authority to investigate money laundering crimes and noncompliance with AML/CTF laws from the HNP to the HCFG. As a result, the ORFK was transferred from the HNP to the HCFG and renamed the CCIB. The FIU no longer performs investigations on its own. STR data is forwarded to the HNP for investigation. This organizational restructuring of the FIU has caused substantial change in its daily operations, due primarily to a large turnover in personnel. In 2008, many senior officials (including the FIU head) and analysts were replaced by newer, less experienced staff from the HCFG. In addition, the Hungarian FIU's Egmont membership was temporarily suspended for three months in early 2008 pending review of the FIU's new operational status. Despite these events, the FIU is currently operating smoothly and exchanging information with counterpart Egmont FIUs.

The FIU serves as the national center for receiving and analyzing STRs and other information regarding potential money laundering or terrorist financing. It is also responsible for disseminating that information to the competent authorities. STR reporting is scheduled to become electronic by the end of 2008, and will include software for risk analysis and statistical data processing. In 2006, the FIU received 9,999 STRs, and opened 193 cases based upon STRs received. From January 1, 2007 until December 15, 2007, the FIU received 9,475 STRs, opened 40 cases, and confiscated 971,681,352 HUF (approximately $5,500,000). Between January 1 and November 27, 2008, the FIU received 9,512 STRs. During this same period, the CCIB opened 12 new criminal money laundering investigations, seized proceeds in the amount of 4,580,479 euro (approximately $6,100,000), and froze a total of 7,037,877 euro (approximately $9,400,000) in proceeds in bank accounts. The FIU also supported 97 ongoing criminal investigations.

The HFSA and other supervisory bodies have started to provide increased outreach and guidance to financial institutions on their reporting obligations. The FIU provides AML/CTF training for the employees of financial institutions and other obliged entities, especially savings banks, in order to improve the quality of STRs filed.

Sections 151-156 of the Hungarian Code of Criminal Procedure, Act 19 of 1998, contain provisions on asset forfeiture. Under these provisions, assets used to commit crimes, that pose a danger to public safety, or that derive from criminal activity, are subject to forfeiture. All property related to criminal activity during the interval when its owner was involved with a criminal organization can be confiscated, unless the owner proves it was acquired legally. In case of suspicious transactions, the FIU freezes the assets and informs the bank whether it will pursue an investigation. In domestic cases, the FIU has 24 hours to inform the bank of its intentions. For nondomestic transactions, the timeframe is extended to 48 hours. A court ruling determines forfeiture and seizure for all crimes, including terrorist financing. The banking community has cooperated fully with enforcement efforts to trace funds and seize and freeze bank accounts. If the owner of the assets requests it, and the FIU approves the request, the frozen assets may be released on the basis of financial need, such as health-related expenses or basic sustenance. An Asset Recovery Unit will soon be established within the HNP Financial Crimes Division. This change will require an amendment to Decree III of 2008 on Jurisdiction of Investigative Authority, and Act CXXX of 2003 on Cooperation between EU Member States in Criminal Matters.

Act IV of 1978, Article 261, criminalizes terrorist acts. Hungary criminalizes terrorism and all forms of terrorist financing with Act II of 2003, which modifies Criminal Code Article 261. Section 261 of the HCC, amended by Section 9 of Act XXVII, states that any person sponsoring activities of a terrorist or a terrorist group by collecting funds or providing material assets or any other support or facilitation faces five to ten years imprisonment. The GOH distributes the updates of the UN designated terrorist lists to obligated entities (2007 Act 108). Additionally, supervised institutions and the general public can access updates to the UN 1373 Sanctions Committee Consolidated List and its equivalent EU list, as well as the list of Specially Designated Global Terrorists designated by the United States pursuant to Executive Order 13224 on the HFSA homepage. Act CLXXX of 2007

establishes the legal framework for freezing assets/funds related to terrorist financing. According to the Act, the FIU examines whether the certain persons and entities subject to the EU's economic and financial restrictive measures have funds or economic resources in Hungary. Act XIX of 1998 on Criminal Procedures, Articles 151, 159, and 160, provide for the immediate seizure, sequestration, and precautionary measures against terrorist assets.

Hungary and the United States have a Mutual Legal Assistance Treaty and a nonbinding information sharing arrangement designed to enable U.S. and Hungarian law enforcement to work more closely to fight organized crime and illicit transnational activities. In May 2000, Hungary and the U.S. Federal Bureau of Investigation established a joint task force to combat Russian organized crime groups. Hungary has signed bilateral agreements with 41 other countries to cooperate in combating terrorism, drug-trafficking, and organized crime.

The GOH is a member of Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), and Hungary's FIU is a member of the Egmont Group. Hungary is a party to the UN Convention for the Suppression of the Financing of Terrorism; the UN Convention against Transnational Organized Crime; the 1988 UN Drug Convention; and the UN Convention against Corruption.

Hungary has strengthened its legal and institutional background and has made significant progress regarding international communication. Despite its progress, the Government of Hungary needs to continue its efforts with regard to implementation. An increased level of cooperation and coordination among the different law enforcement entities involved in fighting financial crime should be pursued. Prosecutors, judges, and police require enhanced knowledge to promote the successful prosecution of money laundering cases, which recent conferences organized by the Prosecution Office have been promoting. The police and FIU should have the option to extend their 24-hour time limit for the freezing of assets. The capacity and knowledge of employees of financial institutions and other obliged entities must be raised to improve the quality of STRs filed, in particular those which may be related to terrorist financing. The GOH also should take steps to strengthen its anti-terrorist financing laws.

India

India's emerging role in regional financial transactions, its large system of informal cross-border money flows, large underground economy, widespread use of hawala, and historically disadvantageous tax administration all contribute to the country's vulnerability to money laundering activities. While most money laundering in India aims to facilitate widespread tax avoidance, criminal activity contributes substantially. Some common sources of illegal proceeds in India are narcotics trafficking, illegal trade in endangered wildlife, trade in illegal gems (particularly diamonds), smuggling, trafficking in persons, corruption, and income tax evasion. Historically, because of its location between the heroin-producing countries of the Golden Triangle and Golden Crescent, India continues to be a drug-transit country. The 2008 terrorist attacks in Mumbai intensified concerns about terrorist financing in India.

India's strict foreign-exchange laws and transaction reporting requirements, combined with the banking industry's due diligence policy, make it increasingly difficult for criminals to use formal channels like banks and money transfer companies to launder money. However, large portions of illegal proceeds are often laundered through "hawala" or "hundi" networks or other informal money transfer systems. Hawala is an alternative remittance system whose deep roots in South Asia make it popular among all strata of Indian society, not only immigrant workers. The hawala system can provide the same remittance service as a bank with little or no documentation, at lower rates and with faster delivery, while providing anonymity and security for its customers. Hawala can also be used to avoid currency or capital flow restrictions and to avoid government scrutiny in financial transactions.

Many Indians, especially among the poor and illiterate, do not trust banks and prefer to avoid the lengthy paperwork required to complete a money transfer through a financial institution.

Historically, in Indian hawala transactions, gold has been one of the most important commodities. There is a widespread cultural demand for gold in India and South Asia. Since the mid-1990s, India has liberalized its gold trade restrictions. In recent years, the growing Indian diamond trade has been considered an important factor in providing countervaluation—a method of "balancing the books" in external hawala transactions. Invoice manipulation is also used extensively to avoid both customs duties, taxes, and to launder illicit proceeds through trade-based money laundering.

The Government of India (GOI) neither regulates hawala dealers nor requires them to register with the government. The Reserve Bank of India (RBI), India's central bank, argues that hawala dealers cannot be regulated since they operate illegally and therefore cannot be registered, easily monitored, and regulated. Indian analysts also note that hawala operators are often protected by politicians and corrupt officials.

According to Indian observers, funds transferred through the hawala market are equal to between 30 to 40 percent of the formal market. The RBI estimates that remittances to India sent through legal, formal channels in 2007-2008 amounted to $42.6 billion. Due to the large number of expatriate Indians in North America and the Middle East, India continues to retain its position as the leading recipient of remittances in the world. According to estimates by the World Bank, in 2007, India overtook China and Mexico to become the top country for remittance inflows.

The Indian government has expanded its regulation of the formal financial sector. In December 2005, the RBI issued guidelines requiring financial institutions, including money changers, to follow "know your customer" (KYC) guidelines and maintain transaction records for the sale and purchase of foreign currency. Foreigners and nonresident Indians (NRIs) are permitted to receive cash payments up to the equivalent of $3,000 or its equivalent in other currencies from moneychangers. Recently, the RBI has been taking additional steps to crack down on unlicensed money transmitters and increase monitoring of nonbank money transfer operations like currency exchange kiosks and wire transfer services.

India has illegal black market channels for selling goods. Smuggled goods such as food items, computer parts, cellular phones, gold, and a wide range of imported consumer goods are routinely sold through the black market. By dealing in cash transactions and avoiding customs duties and taxes, black market merchants offer better prices than those offered by regulated merchants. However, due to trade liberalization, the rise in foreign companies working and investing in India, and increased government monitoring, the business volume in smuggled goods has fallen significantly. In the last 10-15 years, most products previously sold in the black market are now traded through lawful channels.

With tax evasion a widespread problem in India, the GOI is gradually making changes to the tax system. The government now requires individuals to use a personal identification number to pay taxes, purchase foreign exchange, and apply for passports. The GOI also introduced a central value added tax (VAT) in April 2005 which replaced numerous complicated state sales taxes and excise taxes with one national uniform VAT rate. As a result, the incentives and opportunities for entrepreneurs and businesses to conceal their sales or income levels have been reduced. All Indian states have implemented the national VAT mandate.

In the aftermath of the September 11 terrorist attacks in the United States, in January 2003 India joined the global community in addressing concerns about money laundering and terrorist finance by implementing the Prevention of Money Laundering Act (PMLA). The PMLA criminalized money laundering, established fines and sentences for money laundering offenses, imposed reporting and record keeping requirements on financial institutions, provided for the seizure and confiscation of

criminal proceeds, and established a financial intelligence unit (FIU). In July 2005, the PMLA's implementing rules and regulations were promulgated. The legislation outlines predicate offenses for money laundering that are listed in a schedule to the Act. However, the Financial Action Task Force (FATF), an international standard setting body on combating illicit finance, recommends a much larger group of predicate offenses, including organized crime, fraud, smuggling, and insider trading. The FATF has also recommended that India lower the monetary threshold for activity to be considered a crime. Penalties for offenses under the PMLA include imprisonment for three to seven years and fines as high as the equivalent of $12,500. If the money laundering offense is related to a drug offense under the Narcotic Drugs and Psychotropic Substances Act (NDPSA), imprisonment can be extended to a maximum of ten years.

The PMLA mandates that banks, financial institutions, and intermediaries of the securities market (such as stock market brokers) maintain records of all cash transactions (deposits/withdrawals, etc.) exceeding the equivalent of $20,000 and keep a record of all transactions dating back 10 years. All banks and finance companies must report monthly to the FIU a list of all cash transactions (single or linked) of over $20,000 and its equivalent in foreign currencies. All the private banks and most of the larger public banks have also implemented appropriate software to create alerts when the transactions are inconsistent with risk categorization and updated profile of customers. Indian outlets of wire transfer services and casinos have also been ordered to report their transactions every month. Individual cash transactions below the equivalent of $1,000 need not be reported.

The Criminal Law Amendment Ordinance allows for the attachment and forfeiture of money or property obtained through bribery, criminal breach of trust, corruption, or theft, and of assets that are disproportionately large in comparison to an individual's known sources of income. The 1973 Code of Criminal Procedure, Chapter XXXIV (Sections 451-459), establishes India's basic framework for confiscating illegal proceeds. The NDPSA of 1985, as amended in 2000, calls for the tracing and forfeiture of assets that have been acquired through narcotics trafficking and prohibits attempts to transfer and conceal those assets. The Smugglers and Foreign Exchange Manipulators (Forfeiture of Property) Act of 1976 (SAFEMA) also allows for the seizure and forfeiture of assets linked to Customs Act violations. The Competent Authority (CA), within the Ministry of Finance (MOF), administers both the NDPSA and the SAFEMA.

The 2001 amendments to the NDPSA allow the CA to seize any asset owned or used by an accused narcotics trafficker immediately upon arrest. Previously, assets could only be seized after a conviction. Even so, Indian law enforcement officers lack knowledge of the procedures for identifying individuals who might be subject to asset seizure/forfeiture and in tracing assets to be seized. They also appear to lack sufficient knowledge in drafting and expeditiously implementing asset freezing orders. In 2005, pursuant to the NDPSA and with U.S. government funding through its Letter of Agreement (LOA) with India, the CA began training law enforcement officials on asset forfeiture laws and procedures. CA has since held ten asset seizure and forfeiture workshops in New Delhi, Himachal Pradesh, Uttar Pradesh, Rajasthan, Andhra Pradesh, Karnataka and Assam. CA reports that the workshops have led to increased seizures and forfeitures. In 2007, the joint U.S./GOI Project Implementation Committee provided additional funds so that the Competent Authority could expand its training.

One of the GOI's principal provisions in combating money laundering is the Foreign Exchange Management Act (FEMA) of 2000. The FEMA's objectives include establishing controls over foreign exchange, preventing capital flight, and maintaining external solvency. FEMA also imposes fines on unlicensed foreign exchange dealers. Related to the FEMA is the Conservation of Foreign Exchange and Prevention of Smuggling Act (COFEPOSA), which provides for preventive detention in smuggling and other matters relating to foreign exchange violations. The MOF's Directorate of Enforcement (DOE) enforces the FEMA and COFEPOSA. The RBI also plays an active role in the regulation and supervision of foreign exchange transactions.

In April 2002, the Indian Parliament passed the Prevention of Terrorism Act (POTA), which criminalized terrorist financing, among other provisions. In March 2003, the GOI announced that it had charged 32 terrorist groups under the POTA. In July 2003, the GOI arrested 702 persons under the POTA. In November 2004, due to concerns that the overall law permitted overreaching police powers not related to the terrorist financing provisions, the Parliament repealed the POTA and amended the Unlawful Activities (Prevention) Act 1967 (UAPA) to include the POTA's salient elements such as criminalization of terrorist financing.

In October 2008, the Indian Supreme Court ordered lower courts to abide by the decisions of the POTA Central Review Committee. In a May 2005 decision, the Committee recommended that POTA charges be dropped against 131 people accused of setting on fire a train car at the Godhra railway station in the State of Gujarat on February 27, 2002. The incident killed 59 people and sparked widespread communal riots in Gujarat. The Supreme Court October 2008 order may allow the Godhra accused, as well as several POTA detainees in other states, to receive bail

As part of the PMLA mandate, India's financial intelligence unit (FIU) was established in January 2006 to combat money laundering and terrorist financing. The FIU is responsible for receiving, processing, analyzing, and disseminating cash and suspicious transaction reports from financial institutions, banking companies, and intermediaries of the securities market. Over the last three years, the FIU has become fully operational and disseminates report analysis to law enforcement and intelligence agencies to investigate and prevent money laundering and curb financial crimes. The FIU consists of a staff of forty-three officers, headed by an Indian Administrative Service Director of equal rank to a Joint Secretary in the GOI ministries. The FIU has been active in providing relevant financial analysis and money laundering investigative training to its staff members as well as bank officials so that suspicious transaction reports (STRs) are carefully reviewed and efficiently processed.

According to the FIU's Annual Report, which covers March 2007-2008, the FIU received more than 2,733 STRs, of which about 1,396 were shared with relevant law enforcement and intelligence agencies. According to FIU officials, income tax evasion has been readily detected in the STRs and has also led to the arrest of suspected terror operatives. Reporting entities have immunity from civil proceedings for disclosures to the FIU. The FIU also receives threat information and leads from foreign intelligence agencies concerning terrorists, terrorist groups, and international financial crimes information. Cash smuggling reports, which are prepared by the Customs and the Enforcement Directorate, are not disclosed to the FIU but are shared with them indirectly on a need-to-know basis. The FIU Director has authority to levy penalties on reporting entities for noncompliance to the provisions of the PMLA.

The FIU is an independent body reporting directly to the Economic Intelligence Council (EIC), which is headed by the Finance Minister. For administrative purposes, the FIU's operations are supervised by the MOF's Department of Revenue. While the FIU receives processes, analyzes, and disseminates information relating to suspect financial transactions to enforcement agencies and foreign FIUs, the unit does not have criminal enforcement, investigative, or regulatory powers. The FIU maintains regular contact with government departments that receive information about STRs, including the Central Board of Direct Taxes, Enforcement Directorate, Narcotics Control Bureau, and intelligence agencies.

In June 2007, India's FIU was admitted as a member of the Egmont Group. Admission into the Egmont Group is seen by the Indian government as a major step forward by India to join the international community in its fight against money laundering and terrorist financing. The FIU has signed some bilateral MOUs (including with Brazil, Mauritius, and the Philippines) to further facilitate and expedite financial intelligence information sharing. In FY 2007-08, the FIU received requests for information from foreign FIUs for 39 cases and requested information from foreign FIUs in 13 cases.

Under the MOF, the Enforcement Directorate is responsible for investigations and prosecutions of money laundering cases. In 2007-2008, the Enforcement Directorate initiated investigations into 38 cases of money laundering, eight of which were related to terrorist financing. The directorate has made seven seizure cases of properties. Headquartered in New Delhi, the directorate has seven zonal offices in Mumbai, Kolkata, Delhi, Jalandhar, Chennai, Ahmedabad, and Bangalore. In addition to the MOF, the Central Bureau of Investigation (CBI), the Directorate of Revenue Intelligence (DRI), Customs and Excise, RBI, and the CA are involved in GOI's anti-money laundering efforts.

The CBI is a member of INTERPOL. All state police forces and other law enforcement agencies have a link through INTERPOL/New Delhi to their counterparts in other countries for purposes of criminal investigations. India's Customs Service is a member of the World Customs Organization and shares enforcement information with countries in the Asia/Pacific region.

To assist in enhancing coordination among various enforcement agencies and directorates at the MOF, the GOI has established an Economic Intelligence Council (EIC). This provides a forum to strengthen intelligence and operational coordination, to formulate common strategies to combat economic offenses, and to discuss cases requiring interagency cooperation. In addition to the central EIC, there are eighteen regional economic committees in India. The Central Economic Intelligence Bureau (CEIB) functions as the secretariat for the EIC in the MOF. The CEIB interacts with the National Security Council, the Intelligence Bureau, and the Ministry of Home Affairs on matters concerning national security and terrorism.

In October 2006, the MOF started the process to reconcile its list of predicate crimes under the PMLA with that of international FATF recommendations. Having made some progress towards that commitment, India gained FATF observer status in February 2007 with aspirations that in a two-year probationary period it will adopt FATF core recommendations towards gaining full membership. These recommendations focus on meeting international standards for the criminalization of money laundering, customer due diligence, record-keeping, suspicious transaction reporting, criminalization of terrorist financing, and suspicious transaction reporting relating to terrorist financing. India is a member of the Asia/Pacific Group (APG) on Money Laundering, a FATF-style regional body.

The MOF is leading an inter-ministerial effort to amend the PMLA to meet FATF requirements and transition them from observer to full member within this international body. In October 2008, the GOI tabled a bill in Parliament to amend the PMLA. Under the proposed new legislation, insider trading and market manipulation will be treated as a laundering offence and warrant stricter punishment. Offences related to human trafficking, smuggling of migrants, counterfeiting, piracy, environmental crimes, and over-invoicing and under-invoicing under the Customs Act will also be punishable under the PMLA. Credit card payment gateways such as Visa and Mastercard, money changers, money transfer service providers like Western Union, and casinos will also be subject to India's money laundering legislation and face mandatory reporting obligations. Fraud and theft offences have been included as scheduled offences under the PMLA if committed with cross-border implications. The draft legislation also empowers the Enforcement Directorate to "search premises immediately after the offence is committed." The bill also enables the GOI to return the confiscated property to the requesting country in order to implement the provisions of the United Nation's Convention against Corruption. While these amendments to the PMLA broaden the scope of predicate offences and criminalize terrorist financing, the legislation falls short of certain FATF recommendations, including retaining a high value threshold on many of the offenses, unless they are cross-border offenses.

The financial services sector is supervised and regulated by the Reserve Bank of India, the Securities and Exchange Board of India (SEBI), and the Insurance Regulatory and Development Authority (IRDA). SEBI, IRDA, and the National Housing Board have also adopted anti-money laundering policies. SEBI has also issued a circular to all registered intermediaries on their obligations as financial institutions to prevent money laundering. This includes guidelines on maintaining records,

preserving sensitive information with respect to certain transactions, and reporting suspicious cash flows and financial transactions to the FIU. Notably, there is no requirement that SEBI-regulated entities screen collected KYC data, under the presumption that in any noncash transaction, Indian banks have already screened the parties or, if coming from abroad, they have registered with SEBI as a foreign institutional investor.

Prompted by the RBI's 2002 notice to commercial banks to adopt due diligence rules, most of these institutions have taken steps to combat money laundering. For example, most private banks and several public banks have hired anti-money laundering compliance officers to design systems and training to ensure compliance with these regulations. The Indian Bankers Association has also established a working group to develop self-regulatory anti-money laundering procedures and assist banks in adopting the mandated rules.

The RBI and SEBI have worked together to tighten regulations, strengthen supervision, and ensure compliance with KYC norms, which were implemented in December 2005. This includes, for example, provisions that banks must identify politically exposed persons (PEPs) who reside outside of India and identify the source of these funds before accepting deposits of more than $10,000. The RBI continues to update its due diligence guidelines based on FATF recommendations. For banks that are found noncompliant, the RBI has the power to order banks to freeze assets.

Banks have installed software to enable their internal controllers to better monitor accounts for any unusual relationship between the size of the deposit and the turnover in the account and for matching names of terrorists and terrorist-associated countries. All banks have been advised by RBI that they should guard against establishing relationships with foreign financial institutions that permit their accounts to be used by shell companies. No shell bank exists in India nor is permitted to operate under Indian laws. The RBI guidelines impose an obligation on the banks that, as far as reasonably possible, their respondent banks do not offer services to shell institutions.

The financial institutions that operate overseas branches or subsidiaries have been advised to implement the more rigorous anti-money laundering standard—either the Indian law or the host country obligations. Companies are registered under the provisions of the Companies Act and are regulated by the Registrar of Companies. India does not allow bearer shares. Listed companies are subjected to further regulations/restrictions by stock exchanges and supervision of the SEBI. Stock exchanges and other intermediaries are required to comply with the provisions of the PMLA and the rules in respect of client companies.

India does not have an offshore financial center but does license offshore banking units (OBUs). These OBUs are required to be predominantly owned by individuals of Indian nationality or origin resident outside India. The OBUs include overseas companies, partnership firms, societies, and other corporate bodies. OBUs must be audited to confirm that ownership by a nonresident Indian is not less than 60 percent. These entities are susceptible to money laundering activities, in part because of a lack of stringent monitoring of transactions in which they are involved. Finally, OBUs must be audited financially; however, the auditing firm is not required to obtain government approval.

To prevent the abuse of charities for money laundering or terrorism finance, the Foreign Contributions Regulation Act of 1976 requires any nongovernmental entity to register or request permission from the MHA before receiving foreign donations. The government requires registered entities to submit annual reports documenting foreign contributions and their use.

GOI regulations governing charities remain antiquated and the process by which charities are governed at the provincial and regional levels is weak. The GOI does require charities to register with the state-based Registrar of Societies, and, if seeking tax exempt status, they must apply separately with the Exemptions Department of the Central Board of Direct Taxes. There are no guidelines or provisions governing the oversight of charities for anti-money laundering or counterterrorist financing

(AML/CTF) purposes, and there is insufficient integration and coordination between charities' regulators and law enforcement authorities regarding the threat of terrorist finance. The Foreign Contribution Regulation Act (FCRA) of 1976, supervised by the MHA, regulates the use of foreign funds received by charitable/nonprofit organizations.

The Indian government is now considering a proposal to replace the FCRA with the Foreign Contribution Regulation (FCR) Bill of 2006 to regulate existing laws governing contributions from abroad and check the use of foreign funds for subversive activities by terrorist and anti-national organizations. The FCR Bill was introduced in Parliament in December 2006 and then referred to the Parliamentary Standing Committee on Home Affairs for further debate. The bill provides for closer government monitoring, additional registration requirements, and expands the classification of individuals banned from accepting any foreign contribution. Meanwhile, the Parliamentary Standing Committee has recently indicated that the legislation should be amended to define the term "foreign source" more clearly in relation to Indian companies that have more than 50 percent foreign holding. The committee also suggested that companies with foreign holdings over 50 percent should be excluded from the purview of the term in the proposed law.

The UNSCR 1267 Sanctions Committee's consolidated list is routinely circulated to all financial institutions by the RBI, as are other terrorist watch lists adopted by the UN. Prior to the terrorist attacks in Mumbai during late November 2008, India lacked both an adequate legal authority and enforcement mechanism for freezing the funds of terrorist entities. In response to the attacks, India's parliament in December 2008 enacted an amendment to the UAPA containing provisions to address these deficiencies, including an explicit authority to freeze the funds of terrorist entities designated under UNSCR 1373. However, it is too soon to assess the implementation of this amendment and the impact it will have on India's ability to combat terrorism finance.

The GOI is a party to the 1988 UN Drug Convention and the UN Convention for the Suppression of the Financing of Terrorism. It is a signatory to, but has not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. India has signed and ratified a number of mutual legal assistance treaties with many countries, including the United States.

The Government of India should pass the PMLA amendments in Parliament in order to strengthen its AML/CTF regime and to work towards full membership in the FATF. Further steps in tax reform will also assist in negating the popularity of hawala and in reducing money laundering, fraud, and financial crimes. India should become a party to the UN Conventions against Transnational Organized Crime and Corruption. Also, India should pass the Foreign Contribution Regulation Bill for regulating nongovernmental organizations including charities. Given the number of terrorist attacks in India and the fact that in India hawala is directly linked to terrorist financing, the GOI should prioritize cooperation with international initiatives that provide increased transparency in alternative remittance systems. India should devote more law enforcement and customs resources to curb abuses in the diamond trade. It should also consider the establishment of a Trade Transparency Unit (TTU) that promotes trade transparency; in India, trade is the "back door" to underground financial systems. The GOI also needs to strengthen regulations and enforcement targeting illegal transactions in informal money transfer channels.

Indonesia

Although neither a regional financial center nor an offshore financial haven, Indonesia is vulnerable to money laundering and terrorist financing due to gaps in financial system regulation, a cash-based economy, a lack of effective law enforcement, and the increasingly sophisticated tactics of major indigenous terrorist groups, such as Jemaah Islamiya, and their financiers from abroad. Most money laundering in the country is connected to nondrug criminal activity such as gambling, prostitution, bank fraud, theft, credit card fraud, maritime piracy, sale of counterfeit goods, illegal logging, and

corruption. Indonesia also has a long history of smuggling, a practice facilitated by thousands of miles of un-patrolled coastline, weak law enforcement and poor customs infrastructure. The proceeds of illicit activities are easily moved offshore and repatriated as required for commercial and personal needs. Indonesia is emerging from a period marked by weak rule of law and extreme levels of corruption. Corruption remains a very significant issue for all aspects of Indonesian society and a challenge for anti-money laundering and counter terrorism finance (AML/CTF) implementation.

In April 2002, Indonesia passed Law No. 15/2002 Concerning the Crime of Money Laundering, making money laundering a criminal offense. The law identifies 15 predicate offenses related to money laundering, including narcotics trafficking and most major crimes. Law No. 15/2002 established the Financial Transactions Reports and Analysis Centre (PPATK), Indonesia's financial intelligence unit (FIU) to develop policy and regulations to combat money laundering and terrorist financing.

Law No. 15/2002 stipulated important provisions to enhance Indonesia's anti-money laundering (AML) regime, such as: obligating financial service providers to submit suspicious transactions reports and cash transaction reports; exempting reporting, investigation and prosecution of criminal offenses of money laundering from the provisions of bank secrecy that are stipulated in Indonesia's banking law; placing the burden of proof on the defendant; establishing the PPATK as an independent agency with the duty and the authority to prevent and eradicate money laundering; and establishing a clear legal basis for freezing and confiscating the proceeds of crime.

In September 2003, Parliament passed Law No. 25/2003, amending Law No. 15/2002, to address the Financial Action Task Force's (FATF's) concerns about the money laundering situation in the country. Law No. 25/2003 provides a new definition for the crime of money laundering, making it an offense for anyone to deal intentionally with assets known, or reasonably suspected, to constitute proceeds of crime with the purpose of disguising or concealing the origin of the assets. The amendment removes the threshold requirement for proceeds of crime. The amendment further expands the scope of regulations by expanding the definition of reportable suspicious transactions to include attempted or unfinished transactions. The amendment also shortens the time to file a suspicious transactions report (STR) to three days or less after the discovery of an indication of a suspicious transaction.

However, the amendment contains a number of significant deficiencies. The direct and indirect provision of funds to a terrorist organization is not comprehensively covered and there is no clear legal obligation to report STRs related to terrorist financing. In addition, since passage, the ML offence has not yet been used to pursue the proceeds of a wide range of predicate offences. This ineffective implementation is in part due to the narrow scope of the ML offence, as well as the Indonesian government's continuing use of alternative indictments and enforcement capacity issues. The amendment makes it an offense to disclose information about the reported transactions to third parties, which carries a penalty of imprisonment for a maximum of five years and a maximum fine of one billion rupiah (RP) (approximately $85,340).

Additionally, Articles 44 and 44A of Law 25/2003 provide for mutual legal assistance with respect to money laundering cases, with the ability to provide assistance using the compulsory powers of the court. Article 44B imposes a mandatory obligation on the PPATK to implement provisions of international conventions or international recommendations on the prevention and eradication of money laundering. In March 2006, the Government of Indonesia (GOI) expanded Indonesia's ability to provide mutual legal assistance by enacting the first Mutual Legal Assistance (MLA) Law (No. 1/2006), which establishes formal, binding procedures to facilitate MLA with other states.

A proposed second amendment to the AML law was submitted to the parliament in October 2006 and has not yet passed. The amendment would require nonfinancial service businesses and professionals who potentially could be involved in money laundering, such as car dealers, real estate companies, jewelry traders, notaries and public accountants, to report suspicious transactions. The amendments

also would include civil asset forfeiture and give more investigative powers to the PPATK, as well as the authority to block financial transactions suspected of being related to money laundering. Despite these provisions, the draft amendments appear to have remaining gaps when measured against current AML/CTF international standards.

On April 17, 2007, Indonesia adopted a National Strategy 2007-2011 for the prevention and eradication of money laundering. The GOI held two National Coordination Committee meetings in December 2007 and May 2008 to coordinate implementation of the national strategy.

Indonesia's FIU, PPATK, established in April 2002, became operational in October 2003 and continues to make progress in developing its human and institutional capacity. The PPATK is an independent agency that reports directly to the President. The core FIU functions outlined in Article 26 of their anti-money laundering law states that PPATK shall receive, analyze, evaluate and disseminate currency and suspicious financial transaction reports to law enforcement agencies, provide advice and assistance to relevant authorities, and issue publications. In addition, PPATK prepares and offers recommendations to provide direction for national policy in the area of prevention and eradication of money laundering and other serious crimes.

As of December 31, 2008, the PPATK had received a total of 23,056 STRs from banks and nonbank financial institutions. Approximately 11,000 of these STRs were received during 2008. The agency also reported that it had received over 6.3 million cash transaction reports (CTRs) from banks, moneychangers, rural banks, insurance companies, and securities companies. PPATK has submitted a total of 612 cases to various law enforcement agencies based on their analysis of 1,215 STRs.

A number of deficiencies in Indonesia's AML law have resulted in weak customer due diligence (CDD) standards for Indonesian financial institutions. These institutions have no explicit requirement to perform diligence when money laundering or terrorism finance is suspected and there is also no clear provision in the law to prohibit the continuing operation of anonymous accounts. Requirements for confirming whether a person acting on behalf of a legal person is so authorized are also not set out in current laws or regulations.

The 2008 Asia Pacific Group (APG) mutual evaluation of Indonesia notes that since 2004, there have been 176 money laundering investigations, investigations, 19 prosecutions and 11 convictions. Most of the prosecuted money laundering cases have been limited to the proceeds of corruption or fraud. There are few investigations and prosecutions of money laundering cases in parallel with predicate offences. Sentences included imprisonment of up to six to eight years and fines up to IDR 500 million (approximately $42,600).

The Indonesian National Police (POLRI) is the competent authority for investigating money laundering and terrorist finance offenses, while POLRI, the Corruption Eradication Commission (KPK), Customs and various other agencies are responsible for predicate offences. The POLRI, as a matter of priority, has trained a significant number of its officers for AML/CTV. However, given the size of the country and the money laundering and terror finance threat level, POLRI lacks capacity to proactively initiate investigations. Although the POLRI has successfully arrested over 400 terrorists in recent years, the agency has not investigated terrorist financing related to those cases.

The Transnational Crime Coordination Center reports that the POLRI conducted 133 inquiries in 2008 (through September) of financial crimes that have money laundering as an element. PPATK reports there has been one case that has resulted in successful prosecution in 2008. The case, brought in central Jakarta court in January 2008, involved money laundering and banking fraud and included three defendants. The defendants collected funds from customers without a license and were suspected of laundering the fraudulent proceeds. They received sentences ranging from 8-12 years imprisonment and individual fines of Rp 10 billion (approximately $852,700).

The PPATK actively pursues broader cooperation with relevant GOI agencies. The PPATK has signed a total of 22 domestic memoranda of understanding (MOUs) to assist in financial intelligence information exchange with the following entities: Attorney General's Office (AGO), Bank Indonesia (BI), the Capital Market Supervisory Agency—Financial Institutions (BAPEPAM-LK), the Directorate General of Taxation, Director General for Customs and Excise, the Ministry of Forestry Center for International Forestry Research, the Indonesian National Police, the Supreme Audit Board (BPK), the Corruption Eradication Commission, the Judicial Commission, the Directorate General of Immigration, the State Auditor, the Directorate General of the Administrative Legal Affairs Department of Law and Human Rights, the Anti-Narcotics National Board, the Province of Aceh, the Commodity Futures Trading Supervisory Agency, Elections Supervisory Body, Banking University Perbanas Surabaya, University of Surabaya, and Gajah Mada University .

Bank Indonesia (BI), the Indonesian Central Bank, issued Regulation No. 3/10/PBI/2001, "The Application of Know Your Customer Principles," on June 18, 2001. This regulation requires banks to obtain information on prospective customers, including third party beneficial owners, and to verify the identity of all owners, with personal interviews if necessary. The regulation also requires banks to establish special monitoring units and appoint compliance officers responsible for implementation of the new rules and to maintain adequate information systems to comply with the law. Financial institutions and their employees are provided with necessary "safe harbor" provisions for reporting STRs.

BI has issued an Internal Circular Letter No. 6/50/INTERN, dated September 10, 2004 concerning Guidelines for the Supervision and Examination of the Implementation of KYC and AML by Commercial Banks. Bank Indonesia Regulation No. 5/23/PBI/2003 extended their KYC principles to rural banks. In addition, BI also issued a Circular Letter to Commercial Banks No. 6/37/DPNP, dated September 10, 2004, concerning the Assessment and Imposition of Sanctions on the Implementation of KYC and other Obligations Related to Law on Money Laundering Crimes. BI is also preparing Guidelines for Money Changers on Record Keeping and Reporting Procedures, and Money Changer Examinations to be given by BI examiners. Currently, banks must report all foreign exchange transactions and foreign obligations to BI. Similar regulations for nonbank financial institutions have also been implemented. The decree of the head of the Capital Market and Financial Institutions Supervisory Agency No. KEP-313/BL/2007, dated August 28, 2007, amended Regulation No. V.D.10 to strengthen KYC principles.

With respect to the physical movement of currency, Article 16 of Law No. 15/2002 contains a reporting requirement for any person taking cash into or out of Indonesia in the amount of 100 million Rp (approximately $9,370) or more, or the equivalent in another currency, which must be reported to the Director General of Customs and Excise. These reports must be given to the PPATK in no later than five business days and contain details of the identity of the person. Indonesia Central Bank regulation 3/18/PBI/2001 and the Directorate General of Customs and Excise Decree No.01/BC/2005 contain the requirements and procedures of inspection, prohibition, and deposit of Indonesia Rupiah into or out of Indonesia.

The Decree provides implementing guidance for Ministry of Finance Regulation No. 624/PMK. 2004 of December 31, 2004, and requires individuals who import or export more than 100 million Rp in cash (approximately $8,524) to declare such transactions to Customs. This information is to be declared on the Indonesian Customs Declaration (BC3.2). The cash declaration requirements do not cover bearer negotiable instruments as required by FATF's Special Recommendation IX. In addition, cash can only be restrained if the passenger fails to disclose or a false declaration is made. In most cases, the cash is returned to the traveler after a small administrative penalty is applied. There is no clear authority to stop, restrain or seize money that is suspected of promoting terrorism or crime or constitutes the proceeds of crime. As of end-October 2008, the PPATK has received more than 2,764 cross border of cash reports from Customs. The reports were derived from airports in Jakarta and

Denpasar, the seaports of Batam and Tanjung Balai Karimun, Bandung, Batam, Denpasar, Medan and Dumai. Despite these reports, detection and investigative capacity remain weak. As of July 2007, 20 investigations were initiated from cross-border reports. Criminal penalties are limited and are not being applied.

Indonesia's bank secrecy law covers information on bank depositors and their accounts. Such information is generally kept confidential and can only be accessed by the authorities in limited circumstances. However, Article 27(4) of the Law No. 15/2002 expressly exempts the PPATK from "the provisions of other laws related to bank secrecy and the secrecy of other financial transactions" in relation to its functions in receiving and requesting reports and conducting audits of providers of financial services. In addition, Article 14 of the Law No. 15/2002 exempts providers of financial services from bank secrecy provisions when carrying out their reporting obligations. Providers of financial services, their officials, and employees are given protection from civil or criminal action for making required disclosures under Article 15 of the anti-money laundering legislation.

There is a mechanism to obtain access to confidential information from financial institutions through BI regulation number 2/19/PBI/2000. PPATK has the authority to conduct supervision and monitoring compliance of providers of financial services. PPATK may also advise and assist relevant authorities regarding information obtained by the PPATK in accordance with the provisions of this Law No. 15/2002.

The GOI has limited formal instruments to trace and forfeit illicit assets. Under the Indonesian legal system, confiscation against all types of assets must be effected through criminal justice proceedings and be based on a court order. Banking legislation pending with the Indonesian House of Representatives would allow BI to take freezing action on its own authority. BI officials expect this legislation to be approved in 2009. The GOI has no clear legal mechanism to trace and freeze assets of individuals or entities on the UNSCR 1267 Sanctions Committee's consolidated list, and there is no clear administrative or judicial process to implement this resolution and UNSCR 1373. While the BI circulates the consolidated list to all banks operating in Indonesia, this interagency process is too complex and inefficient to send out asset-freezing instructions in a timely manner. In addition, no clear instructions are provided to financial institutions as to what will happen when assets are discovered. Banks also note that without very specific information, the preponderance of similar names and inexact addresses, along with lack of a unique identifier in Indonesia, make identifying the accounts very difficult. Attempts to use a criminal process are confusing and ad hoc at best, and rely on lengthy investigation processes before consideration can be given to freezing or forfeiting assets. Indonesia has a draft asset forfeiture bill, which, if enacted, would give a wide range of powers to investigating officials to identify and trace property.

The PPATK significantly supports the KPK with financial intelligence information. In December 2004 the newly elected President of Indonesia signed a Presidential Instruction to all agencies to intensify efforts in combating corruption in line with their respective functions and roles. The instruction also dictates the establishment of a national Plan of Action combating corruption for the years 2004 through to 2009. The Plan contains three components; namely preventive measures, repressive measures, and monitoring and evaluation, and is seen by the Indonesian authorities as a sustainable and transparent approach to combating corruption in an integrated and coordinated fashion. Indonesia is ranked 126 of 180 countries in Transparency International's 2008 Corruption Perception Index.

Comprehensive figures for assets frozen, seized and/or forfeited are not compiled in a central location. The Corruption Eradication Commission reports that it seized, froze or confiscated assets in corruption-related cases in the amount of 404 billion Rp (approximately $34.5 million) in 2008, through October 31. This compares to assets of 45 billion Rp (approximately $3.8 million) in 2007 and 12.7 billion (approximately $1.1 million) Rp in 2006.

Article 32 of Law No. 15/2002, as amended by Law No. 25/2003, provides that investigators, public prosecutors and judges are authorized to freeze any assets that are reasonably suspected to be the proceeds of crime. Article 34 stipulates that if sufficient evidence is obtained during the examination of the defendant in court, the judge may order the sequestration of assets known or reasonably suspected to be the proceeds of crime. In addition, Article 37 provides for a confiscation mechanism if the defendant dies prior to the rendition of judgment.

In August 2006, the GOI enacted Indonesia's first Witness and Victim Protection Law (No. 13/2006). Members have been chosen in 2008 for a new Witness and Victim Protection Body, established by this law. Indonesia's AML Law and Government Implementing Regulation No. 57/2003 also provide protection to whistleblowers and witnesses. An additional implementing regulation, No. 44/2008, issued May 2008, addressed provision of compensation, restitution and assistance to witnesses and victims. Despite this progress, the lack of an independent budget or dedicated facilities has hampered the newly established body from fulfilling its mandate.

The October 18, 2002 emergency counterterrorism regulation, the Government Regulation in Lieu of Law of the Republic of Indonesia (Perpu), No. 1 of 2002 on Eradication of Terrorism, criminalizes terrorism and provides the legal basis for the GOI to act against terrorists, including the tracking and freezing of assets. The Perpu provides a minimum of three years and a maximum of 15 years imprisonment for anyone who is convicted of intentionally providing or collecting funds that are knowingly used in part or in whole for acts of terrorism. However, the terrorist financing regulation appears to suffer from a number of deficiencies. For example, the terrorist financing offense must be linked to a specific act of terrorism and the prosecution must prove that the offender specifically intended that the funds be used for acts of terrorism. This regulation is necessary because Indonesia's anti-money laundering law criminalizes the laundering of "proceeds" of crimes, but it is often unclear to what extent terrorism generates proceeds. Terrorist financing is therefore not fully included as a predicate for the money laundering offence. In October 2004, an Indonesian court convicted and sentenced one Indonesian to four years in prison on terrorism charges connected to his role in the financing of the August 2003 bombing of the Jakarta Marriott Hotel. The PPATK issued Decision No. Kep. 13/1.02.2/PPATK/02/08, dated February 4, 2008, regarding Guidelines on Identification of Suspicious Financial Transactions related to Terrorism Financing for Financial Service Providers. Indonesia's commitment to overcoming terrorism is evidenced by its success in apprehending terrorists, with 423 arrests and 367 convictions of terrorists in recent years.

There is very weak transparency and governance in the Non Profit Organization (NPO) sector and few measures in place to prevent and detect the abuse of NPOs possibly involved in terror finance. According to the Asia Pacific Group 2008 mutual evaluation, "There is no effective regulation, oversight or supervision of NPOs in Indonesia, either by government agencies or by self regulatory bodies within the NPO sector. Efforts to implement some regulatory controls over the sector have been ineffective. Although the PPATK has reached out to the NPO sector to raise awareness of terror finance risks, NPO regulators have not taken up issues of transparency, good governance and compliance with laws and regulations." Indonesia also has yet to complete a review of its domestic NPO sector, as requested by the APG.

The GOI has begun to take into account alternative remittance systems and charitable and nonprofit entities in its strategy to combat terrorist financing and money laundering. This is an urgently needed development, as large scale unregulated informal remittance channels continue to operate without adequate registration, oversight, and investigations. BI issued circular letter 8/32/DASB on December 20, 2006, requiring registration of nonbank money remitters since January 1, 2007. BI intends to issue another circular in 2008 that will replace this registration system with a licensing system, effective January 1, 2009. Currently 13 nonbank money remitters have registered with BI, and several others have pending registration applications. The PPATK has issued guidelines for nonbank financial service providers and money remittance agents on the prevention and eradication of money laundering

and the identification and reporting of suspicious and other cash transactions. The PPATK issued Decision no. KEP-47/1.02/PPATK/06/2008, dated June 2, 2008, regarding Guidelines on the Identification of High Risk Products, Customers, Business and Countries for Financial Service Providers. The GOI has initiated a dialogue with charities and nonprofit entities to enhance regulation and oversight of those sectors.

BI also issued the following provisions concerning money changers to improve implementation of Recommendation 5 on Customer Due Diligence and Record Keeping: BI Regulation No. 9/11/PBI/2007, dated September 5, 2007; BI Circular Letter No. 9/23/DPM, dated October 8, 2007, concerning the permit procedure, implementation of KYC principles, supervision, reporting and imposition of sanctions for nonbank money changers; BI Circular Letter No. 9/36/DPND, dated December 19, 2007, concerning the permit and reporting procedures for banks which perform business activity as money changers; and BI Circular Letter No. 9/38/DPBPR, dated December 28, 2007, concerning the permit and reporting procedure for rural banks and sharia rural banks which perform business activity as money changers. PPATK and BI carried out an authorized money changer awareness campaign during the second half of 2007 and the first half of 2008, in collaboration with the Millennium Challenge Corporation Threshold Program and USAID.

BI has effective legal powers and policies in place to ensure that shell banks are not permitted, although there is no explicit legislative prohibition on establishing a shell bank in Indonesia. The bank licensing procedures followed by BI effectively precludes establishment of a shell bank and BI Regulation 3/10/PBI/2003 as amended by 5/21/PBI/2002 provides that banks in Indonesia are required to refuse to open an account and/or conduct transactions with any prospective customer incorporated as a shell bank.

Bearer shares appear to remain a feature of the Indonesian financial system, as the law previously permitted both bearer and registered shares. The new Limited Liability Company Law (Law 40/2007), August 16, 2007, prohibits bearer shares. This provision, in conjunction with the new Investment Law, prevents parties from making nominee arrangements. Complete implementing regulations have not yet been issued for the new law and the process for removing bearer shares from the system is not clear. Previously issued bearer shares appear to remain valid.

The GOI has established special economic zones to attract both foreign and domestic investment. In 2007, the House of Representatives approved establishment of free trade zones (FTZs) in the Batam, Bintan and Karimun islands. The GOI established a Batam- Bintan- Karimun Free Trade Zone Council and has made preparations for the implementation of free trade zone regulations. Batam Island, located just south of Singapore, has long been a bonded zone in which investment incentives have been offered to foreign and domestic companies. In 2007, 973 domestic companies, foreign companies and joint ventures had invested more than $1 billion in the zone. Numerous Indonesian authorities perform supervision over firms located in the special economic zones (the Investment Coordinating Board, the Ministry of Laws and Human Rights, the Ministry of Manpower, the Ministry of Finance). Supervision includes confirming identities of investors. In Batam, other authorities exercising supervision include the Batam Industrial Development Authority and the Municipality of Batam. The GOI is currently in the process of drafting regulations providing wider authority for Customs & Excise officials to regulate the flow of goods through the new Batam FTZ, given the FTZ's vulnerability to smuggling.

Indonesia is an active member of the Asia/Pacific Group on Money Laundering (APG), and in 2008 served as the co-chair. The APG conducted its second mutual evaluation of Indonesia in November 2007 and the report was discussed and adopted at the APG Annual Meeting in July 2008. In June 2004, PPATK became a member of the Egmont Group. The PPATK has pursued broader cooperation through the MOU process and has concluded 27 MOUs, 25 of which were with other Egmont FIUs. The PPATK has also entered into an Exchange of Letters enabling international exchange with Hong

Kong. Indonesia has signed Mutual Legal Assistance Treaties with Australia, China and South Korea. Indonesia joined other ASEAN nations in signing the ASEAN Treaty on Mutual Legal Assistance in Criminal Matters on November 29, 2004, though the GOI has not yet ratified the treaty. The Indonesian Regional Law Enforcement Cooperation Centre was formally opened in 2005 and was created to develop the operational law enforcement capacity needed to fight transnational crimes.

The GOI has enacted Law No. 7/2007 to implement the 1988 UN Drug Convention, to which Indonesia is a party. The GOI also has enacted Law No. 22/1997 Concerning Drugs and Psychotropic Substances, which makes the possession, purchase or cultivation of narcotic drugs or psychotropic substances for personal consumption a criminal offense. Indonesia is a party to the UN Convention for the Suppression of the Financing of Terrorism and a party to the UN Convention against Corruption. The GOI has signed but has yet to ratify the UN Convention against Transnational Organized Crime.

The Government of Indonesia has made progress in constructing an AML regime. However, despite the continuing threat of terrorism in the country and numerous arrests related to terrorism, efforts to combat terrorist financing have been weak and should be strengthened. Sustained public awareness campaigns, new bank and financial institution disclosure requirements, and the PPATK's support for Indonesia's first credible anticorruption drive has led to increased public awareness of financial crimes. Increased prosecution of high-profile corruption cases in 2008 was an important advance in the GOI's efforts to eradicate pervasive corruption. Further investment in human and technical capacity and greater interagency cooperation are needed to develop a truly effective anti-money laundering regime. Authorities should ensure that the PPATK is able to have access, directly or indirectly, to required financial, administrative and law enforcement information on a timely basis. Indonesian police and customs authorities should be encouraged to initiate money laundering investigations at the "street level" and not be dependent on financial intelligence filed with the PPATK. Law enforcement agencies should systematically investigate money laundering in parallel with their investigations of predicate offenses. The highest levels of GOI leadership should continue to demonstrate strong support for strengthening Indonesia's anti-money laundering regime. For example, Indonesia has not established comprehensive controls or oversight over the provision of wire transfers. This is a significant shortcoming in preventative measures for the financial system. Indonesia's cross-border currency declarations should also cover bearer negotiable instruments. Considerably more enforcement is needed to protect Indonesia's extraordinarily long and porous borders. Indonesia should establish clear legal mechanisms and administrative or judicial processes to trace and freeze assets of entities included on the UNSCR 1267 Consolidated List and to implement its obligations under UNSCR 1373. The GOI must continue to improve capacity and interagency cooperation in analyzing suspicious and cash transactions, investigating and prosecuting cases, and achieving deterrent levels of convictions. As part of this effort, Indonesia should review and streamline its process for reviewing UN designations and identifying, freezing and seizing terrorist assets, and become a party to the UN Convention against Transnational Organized Crime.

Iran

Iran is not a regional financial center, but does have a large free trade zone on Kish Island. Iran's economy is marked by a bloated and inefficient state sector and over-reliance on the petroleum industry. Large oil and gas reserves provide 85 percent of government revenue, and state-centered policies have caused major distortions in the economy. A combination of price controls and subsidies continue to weigh down the economy, and, along with widespread corruption, have undermined the potential for private sector-led growth. High oil prices in recent years have enabled Iran to amass nearly $70 billion in foreign exchange reserves, but the economy only experienced moderate growth during this period and is vulnerable to a sustained drop in the value of oil.

After the Iranian Revolution of 1979, the Government of Iran (GOI) nationalized the country's banks. Today, Iran's state-owned banks include Bank Refah, Bank Melli Iran, Bank Saderat, Bank Tejarat, Bank Mellat, Bank Sepah, Bank Kargoshaee, Export Development Bank of Iran, and Post Bank of Iran, as well as three specialized institutions, Bank Keshavrzi, Bank Maskan and Bank of Industry and Mines. Iran has established an international banking network, with many large state-owned banks establishing foreign branches in Europe, the Middle East, and Asia. In 1994, Iran authorized the creation of private credit institutions. Licenses for these banks were first granted in 2001. Currently, these banks include Karafarin, Parsian, Saman Eghtesad, Pasargad, Sarmayeh, and Eghtesade Novin.

In 1984, the Department of State designated Iran as a state sponsor of international terrorism. Iran continues to provide resources and guidance to multiple terrorist organizations and has worked to thwart stability in Iraq. Hamas, Hizballah, and the Palestinian Islamic Jihad (PIJ) maintain representative offices in Tehran in part to help coordinate Iranian financing and training.

On October 11, 2007, the FATF released a statement of concern that "Iran's lack of a comprehensive anti-money laundering/counterterrorist finance regime represents a significant vulnerability within the international financial system." The FATF has subsequently issued three additional statements, the most recent of which was released on October 16, 2008. The statement expressed concerns that Iran's failure to "to address the risk of terrorist financing continues to pose a serious threat to the integrity of the international financial system" and urged all jurisdictions to "strengthen preventive measures to protect their financial sectors."

In a number of cases, Iran has used its state-owned banks to channel funds to terrorist organizations. For example, between 2001 and 2006, Bank Saderat transferred $50 million from the Central Bank of Iran through Bank Saderat's subsidiary in London to its branch in Beirut for the benefit of Hizballah fronts that support acts of violence. Hizballah also used Bank Saderat to send funds to other terrorist organizations, including Hamas, which itself had substantial assets deposited in Bank Saderat as of early 2005.

Elements of Iran's Islamic Revolutionary Guard Corps (IRGC) have been directly involved in the planning and support of terrorist acts throughout the world, including in the Middle East, Europe and Central Asia, and Latin America. The IRGC-Qods Force, which has been designated by the U.S. Department of the Treasury under Executive Order 13224 for providing material support to the Taliban and other terrorist groups, is the Iranian regime's primary mechanism for cultivating and supporting terrorist and militant groups abroad. Qods Force-supported groups include: Lebanese Hizballah; Palestinian terrorists; certain Iraqi Shi'a militant groups; and Islamic militants in Afghanistan and elsewhere. The Qods Force is especially active in the Levant, providing Lebanese Hizballah with funding, weapons and training. It has a long history of supporting Hizballah's military, paramilitary and terrorist activities, and provides Hizballah with more than $100 to $200 million in funding each year. The Qods Force continues to provide the Taliban in Afghanistan with limited weapons, funding, logistics and training in support of anti-U.S. and anti-coalition activities.

Iran's defiance of the international community over its nuclear program and the role of Iranian banks in facilitating proliferation activity have also led to a number of international multilateral actions on Iran's financial sector. Since July 2006, the United Nations Security Council (UNSC) has passed five related resolutions, three of which call for financial restrictions on Iran.

Numerous countries around the world have restricted their financial and business dealings with Iran in response to both the UNSC measures on Iran's nuclear development and proliferation activities, as well as the FATF statements on Iran's lack of adequate AML/CTF controls. Many of the world's leading financial institutions have essentially stopped dealing with Iranian banks, in any currency, and Iranian companies and businesses are facing increased difficulty in obtaining letters of credit.

In addition, some jurisdictions, including the United States, the European Union (EU), and Australia have adopted preventive measures beyond the UNSCRs and FATF statements towards safeguarding against illicit finance threats from Iran. The U.S. Department of the Treasury has designated four Iranian banks (Banks Sepah, Melli, Mellat, and the Export Development Bank of Iran) under Executive Order (E.O.) 13382 for supporting proliferation. An additional bank, Iran's Bank Saderat, was designated by Treasury under E.O. 13224 for providing financial services to the terrorist groups Hizballah, Hamas, and PIJ. Treasury's Financial Crimes Enforcement Network (FinCEN) in both October 2007 and March 2008 issued advisories on the risk to the international financial system posed by Iranian financial institutions, as warned by the FATF. Most recently, in November 2008, Treasury revoked the license authorizing "U-turn" transfers involving Iran, thus terminating Iran's ability to access the U.S. financial system indirectly via non-Iranian foreign banks.

The EU in June 2008 imposed sanctions on Bank Melli (Iran's largest bank) that froze its Europe-based assets and prevented it from doing business in EU states. The EU also imposed a heightened financial monitoring requirement on all transactions involving Bank Saderat. On October 15, 2008, Australia announced sanctions on Banks Melli and Saderat that similarly prevented both banks from doing business with Australian entities.

It has been a standard practice for Iranian financial institutions to conceal their identity to evade detection when conducting transactions. For example, Bank Sepah has requested that its name be removed from transactions in order to make it more difficult for intermediary financial institutions to determine the true parties to a transaction. In addition, when Iranian assets were targeted in Europe, branches of Iranian state-owned banks in Europe took steps to disguise ownership of assets on their books in order to protect assets from future actions. The Central Bank of Iran (CBI), the sole Iranian entity that regulates all Iranian banks, has not only engaged in deceptive practices itself—such as asking for its name to be removed from transactions—but has also encouraged such practices among Iran's state-owned banks. Further, between January and March 2008, the Central Bank of Iran handled tens of millions of dollars in transactions to and from the accounts of U.S. and UN-designated banks held at the CBI.

Illicit finance threats stemming from Iran are not limited to Iran's use of the international financial system, but are also prevalent inside the jurisdiction, itself. Iran has a large underground economy, spurred by restrictive taxation, widespread smuggling, currency exchange controls, capital flight, and a large Iranian expatriate community. The World Bank reports that about 19 percent of Iran's GDP pertains to unofficial economic activities. Reportedly, a prominent Iranian banking official estimates that money laundering encompasses an estimated 20 percent of Iran's economy. Other reports have found that approximately $12 billion is laundered annually via smuggling commodities in Iran and another $6 billion laundered by international criminal networks.

Iran's "bonyads," or charitable religious foundations, were originally established at the time of the Iranian revolution to help the poor. They have rapidly expanded beyond their original mandate. Although still funded, in part, by Islamic charitable contributions, today's bonyads monopolize Iran's import-export market as well as major industries including petroleum, automobiles, hotels, and banks. Bonyad conglomerates account for a substantial percentage of Iran's gross national product. Individual bonyads such as Imman Reza Foundation and the Martyrs' Foundation have billions of dollars in assets. Mullahs direct the bonyad foundations. Given the low rate of capital accumulation in the Iranian economy, the foundations constitute one of the few governmental institutions for internal economic investment. Reportedly, the bonyads stifle entrepreneurship, as the bonyads enjoy favored status, including exemption from taxes, the granting of favorable exchange rates, and lack of accounting oversight by the Iranian government.

On October 25, 2007, the United States designated Iran's Revolutionary Guards Corps (IRGC—the armed guardian of Iran's theocracy) as a proliferator of weapons of mass destruction, and the elite

Qods Force as a supporter of terrorism. The Revolutionary Guard's suspect financing is entwined with Iran's economy. The Revolutionary Guard is involved with more than 100 companies and manages billions of dollars in business. Similar to bonyads, the military/business conglomerate uses high-level political connections, no-bid contracts, and squeezes out competitors. Corruption is widespread throughout Iranian society; at the highest levels of government, favored individuals and families benefit from "baksheesh" deals. Iran is ranked 141 out of 180 countries listed in Transparency International's 2008 Corruption Perception Index. Despite some limited attempts at reforming bonyads and other entities, there has been little transparency or substantive progress.

Via a transit trade agreement, goods purchased primarily in Dubai are sent to ports in southern Iran and then via land routes to markets in Afghanistan. This transit trade facilitates the laundering of Afghan narcotics proceeds via barter transactions, trade-based money laundering, and trade goods that provide counter valuation in the regional hawala markets. According to the United Nations Office on Drugs and Crime, approximately 60 percent of Afghanistan's opium is trafficked across Iran's border. Reportedly, Iran has an estimated three million drug users and the highest per capita heroin addiction rate in the world. Opiates not intended for the Iranian domestic market transit Iran to Turkey, where the morphine base is converted to heroin. Heroin and hashish are delivered to buyers located in Turkey. The drugs are then shipped to the international market, primarily Europe. In Iran and elsewhere in the region, proceeds from narcotics sales are sometimes exchanged for trade goods via value transfer. The United Nations Global Program against Money Laundering (GPML) also reports that illicit proceeds from narcotics trafficking are used to purchase goods in the domestic Iranian market and then the goods are often exported and sold in Dubai.

Iran's real estate market is often used to launder money. Frequently, real estate settlements and payment are made overseas. In addition, there are reports that a massive amount of Iranian capital has been invested in the United Arab Emirates, particularly in Dubai real estate. Reportedly, Iranian investments in Dubai may be in excess of U.S. $350 billion.

A new Iranian money laundering law was approved by the Islamic Parliament on January 22, 2008 and the Guardian Council on February 6, 2008. The law creates a High Council on Anti-Money Laundering chaired by the Minister of Economic Affairs and Finance. Membership in the High Council includes the Ministers of Commerce, Intelligence, Interior, and the Governor of the Central Bank of Iran. The High Council would serve to coordinate and collect information and evidence concerning money laundering offenses, but an operational Financial Intelligence Unit (FIU)—High Council or otherwise—has yet to be established. Nonetheless, the new anti-money laundering law falls significantly short of meeting international standards, particularly with respect to the lack of a corresponding effort to address the risk of terrorism finance emanating from Iran.

According to reports, any individual or business engaging in transfers or transactions of foreign currency into or out of Iran must abide by Central Bank of Iran regulations, including registration and licensing. The regulations and circulars address money transfer businesses, including hawaladars; however, Iran's merchant community makes active use of hawala and moneylenders. Counter valuation in hawala transactions is often accomplished via trade, thus trade-based money laundering is likely a prevalent form of money laundering. Many hawaladars and traditional bazaari are linked directly to the regional hawala hub in Dubai. Over 400,000 Iranians reside in Dubai, with approximately 7,500 Iranian-owned companies based there.

Iran is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. Iran is not a signatory to the UN Convention for the Suppression of the Financing of Terrorism.

The Government of Iran has engaged with the FATF and should vigorously pursue the implementation of a viable anti-money laundering and terrorist finance regime, including effective legislation and proper regulations that adhere to international standards and seeks to address the risk of terrorism

finance emanating from Iran. Above all, the GOI should cease its financial and material support of terrorist organizations and terrorism, as well as its abuse of the international financial system to facilitate proliferation. Iran should be more active in countering regional smuggling. Iran should implement meaningful reforms in bonyads that promote transparency and accountability. Iran should create an anticorruption law with strict penalties and enforcement, applying it equally to figures with close ties to the government, ruling class, business leaders, and the clerical communities. Iran should become a party to the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the UN Convention for the Suppression of the Financing of Terrorism.

Iraq

Iraq's economy is primarily cash-based, and there is little data available on the extent of money laundering in the country. Smuggling is endemic, involving consumer goods, cigarettes, and petroleum products. Bulk cash smuggling, counterfeit currency, trafficking in persons, and intellectual property rights violations are also major problems. There is a large market in Iraq for stolen automobiles from Europe and the United States. Ransoms from kidnappings and extortion cost Iraqi citizens millions of dollars each year, and the funds are often used to finance terrorist networks. Trade-based money laundering, customs fraud, and value transfer are found in the underground economy. Hawala networks, both licensed and unlicensed, are widely used for legitimate and illegitimate purposes. There is little regulation and supervision of the formal and informal financial sectors, resulting in weak internal private sector controls. Under its Stand-by Arrangement with the International Monetary Fund, the Central Bank of Iraq (CBI) has completed half of the necessary prudential regulations and is to finalize the remainder, including anti-money laundering regulations.

Oil production is the main source of revenue for the Iraqi government, but theft and diversion of oil products to the black market are pervasive. In 2006, the World Bank and the Iraqi Ministry of Oil's Office of Inspector General estimated that the Iraqi government loses tens of millions of dollars each year to the smuggling or diversion of refined oil products. In 2006 the State Department estimated that up to 10 percent of the refined petroleum products produced in Iraq are diverted to the black market or smuggled out of Iraq and sold for a profit. At one point in 2007 the diversion of refined petroleum products produced at the Baiji Oil Refinery was so prevalent that the Pentagon estimated that up to 70 percent of the fuel processed there was lost to the black market. It's believed that the funds generated by this criminal activity, possibly as much as $2 billion a year, went toward payments to corrupt officials, funding insurgent activities, and other criminal activities. Consequently, the Iraqi Army, supported by Coalition Forces, began "Operation Honest Hands" on February 12, 2007, and assumed control of security at the Baiji oil refinery complex. Within a few months of the start of the operation, the number of daily tanker loads recorded as shipped by the refinery increased from 20 to 200 per day. Nonetheless, the Baiji Oil Refinery remains a significant money laundering and terrorist financing threat.

Fraudulent investment schemes are also on the rise in Iraq. For example, in 2008 there was an investment scam in the Basra area that netted the perpetrator tens of millions of dollars in a "Ponzi" scheme involving a fake investment company promising investors huge returns of between 200 to 300 percent every six months. When the scheme collapsed, the owner of the investment company fled Iraq with the remaining money.

Corruption is pervasive and impacts all facets of Iraqi society, government, and institutions. The high level of corruption in Iraq poses threats to the developing Iraqi financial system as it facilitates money laundering and the financing of terrorism. Transparency International's 2008 International Corruption Perception index ranked Iraq as 178 out of 180 countries surveyed, demonstrating no change from the previous year. However, Iraq is taking demonstrable steps to combat corruption, including acceding to the UN Convention Against Corruption, ratifying the Extractive Industries Transparency Initiative,

and removing corrupt or incompetent Inspectors General from their positions. Iraq does not have a Mutual Legal Assistance Treaty with the United States and U.S. law enforcement agencies indicate that cooperation with Iraqi counterparts had been somewhat sporadic but is increasing.

The Coalition Provisional Authority (CPA), the international body that governed Iraq beginning in April 2003, issued regulations and orders that carried the weight of law in Iraq. The CPA ceased to exist in June 2004, at which time the Iraqi Interim Government assumed authority for governing Iraq. Drafted and agreed to by Iraqi leaders, the Transitional Administrative Law (TAL) described the powers of the Iraqi government during the transition period. Under TAL Article 26, regulations and orders issued by the CPA pursuant to its authority under international law remain in force until rescinded or amended by legislation duly enacted and having the force of law. The constitution, which was ratified in October 2005, also provides for the continuation of existing laws, including CPA regulations and orders that govern money laundering.

CPA Order No. 93, the "Anti-Money Laundering Act of 2004" (AMLA), governs financial institutions in connection with: money laundering; financing of crime; financing terrorism; and the vigilance required of financial institutions regarding financial transactions. The law also criminalizes money laundering, financing crime (including the financing of terrorism), and structuring cash transactions to avoid legal requirements. The AMLA covers: banks; investment funds; securities dealers; insurance entities; money transmitters; and foreign currency exchange dealers as well as persons who deal in financial instruments, precious metals or gems, and persons who undertake hawala transactions. Covered entities are also required to verify the identity of non-account holders performing a transaction or series of transactions whose value is equal to or greater than five million Iraqi dinars (approximately $4,250). Beneficial owners must be identified upon account opening and for transactions exceeding ten million Iraqi dinars (approximately $8,500). Records must be maintained by financial institutions for a period of at least five years. Covered entities must report suspicious transactions and wait for guidance before proceeding with the transaction; the relevant funds are frozen until guidance is received. Reports of suspicious transactions are to be completed for any transaction over four million Iraqi dinars (approximately $3,400) that are believed to involve funds that are derived from illegal activities or money laundering, intended for the financing of crime (including terrorism), or over which a criminal organization has disposal power, or a transaction conducted to evade any law or which has no apparent business or other lawful purpose. The "tipping off" of customers by bank employees where a transaction has generated a report of suspicious transaction is prohibited. Bank employees are protected from liability for cooperating with the government. Willful violations of the reporting requirement may result in fines or imprisonment.

CPA Order No. 94, the "Banking Law of 2004," gives the CBI the authority to conduct due diligence on proposed bank management. Order No. 94 establishes requirements for bank capital, confidentiality of records, audit and reporting requirements for banks, and prudential standards. The CBI is responsible for the supervision of financial institutions. The CBI was mandated by the AMLA to issue regulations and require financial institutions to provide employee training, appoint compliance officers, develop internal procedures and controls to deter money laundering, and establish an independent audit function. The CBI has branches in Irbil, Sulaymaniyah, Mosul, and Basra.

The CBI headquarters in Baghdad also houses Iraq's financial intelligence unit, the Money Laundering Reporting Office (MLRO). The MLRO is responsible for the collection and analysis of suspicious transactions and forwards the results of their analysis to law enforcement authorities. The MLRO's primary Iraqi law enforcement contact is with the Ministry of Interior's Financial Crimes Unit. The CBI branches are responsible for the licensing and examining of public and private banks, and the licensing of money exchangers and money transmitters. The CBI is required to conduct examinations of public banks every six months and private banks every three months. Order No. 94 gives the CBI administrative enforcement authority including the removal of institution management and revocation of bank licenses. While the banks ostensibly provide traditional banking services such as lending to

the community, in practice they collect funds and send the excess reserves to the CBI in Baghdad where they receive, as of late 2008, a 15 percent return on the deposits. There is no time limit for funds to be held in the CBI for accrual of interest. Outside of this relationship, there is poor communication between the CBI and Iraq's public and private banks, particularly with respect to money laundering, terrorist financing, and other potential risks. The formal financial sector continues to develop. Approximately 33 private banks and seven state-owned banks are operating in Iraq. The state-owned banks still control a majority of the banking sector.

The CBI is still experiencing challenges with communications between its various offices. Efforts are underway to modernize the banking technology utilized by the CBI, but the effort has borne little fruit to date. In particular there is a lack of an adequate electronic payment and wire transfer systems. Electronic payment systems are being introduced in Iraq, including payment of pensions by a "Smart Card" (embedded microchip) and electronic transfers by private banks, but these programs are at an early stage. There is little institutional knowledge in the CBI regarding implementing Iraq's anti-money laundering/countering the financing of terrorism (AML/CTF) legislation and combating systemic money laundering and terrorist finance threats. In addition, the economy is still largely cash-based. The CBI faces lingering societal distrust of banks by the Iraqi people based on their experiences during the Saddam Hussein regime.

Bulk cash smuggling is a significant problem in Iraq. The CBI is considering issuance of regulations to require currency transaction reports be filed for the cross-border transfer of currency in amounts exceeding 15 million Iraqi dinars (approximately $12,750). Neither Iraqis nor foreigners are permitted to carry more than $10,000 in U.S. currency when exiting Iraq. Overseas currency speculation regarding the new Iraqi dinar is widespread often involving fraudulent schemes. It is illegal under Iraqi law to export dinars. Another vulnerability to Iraq's AML/CTF regime is that money exchangers and money transmitters, including hawaladars, are largely unregulated. Because of the efficiency and easy access of the money exchange business and money transmitters, most people in Iraq use these businesses to conduct international business. Some conventional banks can take weeks or months to conduct simple funds transfers while similar international transactions can be done rapidly and efficiently through the informal money exchange and transfer services. Although money exchangers and transmitters are required to be licensed by the CBI, the level of supervision and enforcement is minimal. Money exchangers are not subject to the same level of supervision as banks nor are they required to report suspicious transactions to the CBI. The level of training on AML/CTF given by the CBI to managers and operators of money exchanges and money transmitter businesses is inadequate. The MLRO, in its present form, is unable to provide adequate training and guidance on AML/CTF issues to the banking institutions it oversees, let alone the money transmitter or money exchange businesses in Iraq. Because the MLRO is part of the CBI, it also suffers from the same shortcomings as the CBI regarding communication with the CBI branches outside of Baghdad and the private banks. Furthermore, the MLRO has no criminal investigative authority.

The MLRO, which was formed in mid-2006, is weak and requires significant funding, support and training in order to adequately monitor the formal and informal financial systems in Iraq. The MLRO is understaffed with only 29 personnel, who have rudimentary accounting capabilities and computer skills. Additionally, the MLRO's computer equipment is outdated and access to the internet and the appropriate software is inadequate. The MLRO receives little support from the Iraqi law enforcement agencies. Although, the MLRO is empowered to exchange information with other Iraqi and foreign government agencies, those contacts are limited. All financial institutions in Iraq are required to report suspicious financial transactions, including potential money laundering and terrorist financing, but only a few reports have been submitted since the MLRO's establishment.

The predicate offenses for the crime of money laundering extend beyond "all serious offenses" to include "some form of unlawful activity." The penalties for violating the AMLA depend on the specific nature of the underlying criminal activity. For example, "money laundering" is punishable by

a fine of up to 40 million dinars (approximately $34,000) or twice the value of the property involved in the transaction, (whichever is greater) or imprisonment of up to four years or both. Other offenses for which there are specific penalties include the financing of crime with a fine of up to 20 million dinars (approximately $17,500) or two years imprisonment or both and structuring transactions to avoid reporting requirements of up to 10 million dinars (approximately $8,500) or one year imprisonment or both. No arrests or prosecutions for crimes covered under the AMLA have been reported.

The AMLA includes provisions for the forfeiture of any property. Such property includes, but is not limited to, funds involved in a covered offense, or property traceable to the property, or any property gained as a result of such an offense, without prejudging the rights of bona fide third parties. The courts can order confiscation of property, but they can only do so if the property is directly related to the crime, including drug proceeds. According to the Iraqi Penal Code, a person must pay the government back for any property stolen from the government. In other cases of theft, restitution is made to the victim(s). Any property forfeited to the state becomes state property and goes into the general treasury. Should the government confiscate perishables, it can sell them while the case is ongoing and if the defendant is acquitted, the government returns the money it acquired from the sale of the goods to the defendant. While the case is ongoing, the government appoints a judicial guardian to supervise and maintain the property pending the outcome of the case. The AMLA also blocks any funds or assets, other than real property (which is covered by separate regulation) belonging to members of the former Iraqi regime and authorizes the Minister of Finance to confiscate such assets following a judicial or administrative order. The lack of automation or infrastructure in the banking sector hinders the government's ability to identify and freeze assets linked to illicit activities.

Iraq has four free trade zones: the Basra/Khor al-Zubair seaport; Ninewa/Falafel area; Sulaymaniyah; and al-Qaim, located in western Al Anbar province. Under the Free Trade Zone (FZ) Authority Law, goods imported or exported from the FZ are generally exempt from all taxes and duties, unless the goods are to be imported for use in Iraq. Additionally, capital, profits, and investment income from projects in the FZ are exempt from taxes and fees throughout the life of the project, including the foundation and construction phases. Value transfer via trade goods is a significant problem in Iraq and the surrounding region

The CBI distributes the UN 1267 Sanction Committee's consolidated list of suspected terrorist organizations to the various banks under its supervision as mandated by the AMLA. However, no asset seizures or any other information pertaining to the names on this list has been reported. Currently there is no legislation in Iraq that allows the GOI to freeze and confiscate terrorist assets without delay under civil proceedings. This represents a significant shortfall in the GOI's AML/CTF regime and in the international standards set by the Financial Action Task Force (FATF)

Iraq became a member of the Middle East and North Africa Financial Action Task Force (MENAFATF) in September 2005. However, neither representatives from the MLRO nor the CBI have attended a MENAFATF plenary meeting or its training workshops since 2007. Iraq also has not yet undergone a mutual evaluation of its compliance with the FATF standards. Iraq is a party to the 1988 UN Drug Convention, the UN Convention against Corruption, and the UN Convention against Transnational Organized Crime. It is not a party to the UN Convention for the Suppression of the Financing of Terrorism.

The Government of Iraq has the foundation needed to support the fight against terrorist financing and money laundering, but needs to implement existing legislation, bolster the relevant agencies in Iraq's AML/CTF regime, and issue or establish the proper regulations and legislation related to combating systemic money laundering and terrorist financing threats in Iraq. The CBI should be particularly cautious about granting licenses to banks from jurisdictions of concern; the MLRO needs proper training, equipment, and direction; the Iraqi financial sector needs to adopt and use AML/CTF

standards and best practices; the GOI should pass legislation that allows Iraq to freeze and confiscate terrorist assets; Iraq needs to participate fully in the MENAFATF by attending its plenary meetings, taking advantage of its training opportunities and implementing the FATF's international standards; Iraqi law enforcement and the judiciary need to enhance their ability to soundly interpret, apply, and enforce the legal principles of the AMLA and therefore better conduct investigations; Iraqi law enforcement, border authorities, and customs service should continue to strengthen border enforcement and identify and pursue smuggling, trade-based money laundering, and terrorist financing networks; and, the GOI should make a concerted effort to combat the corruption that hinders development and impedes an effective anti-money laundering and counterterrorist financing regime. Iraq should become a party to the UN Convention for the Suppression of the Financing of Terrorism.

Ireland

Ireland is an increasingly significant European financial hub. Narcotics-trafficking, fraud, and tax offenses are the primary sources of funds laundered in Ireland. Money laundering occurs in credit institutions, although launderers have also made use of money remittance companies, solicitors, accountants, and second-hand car dealerships. The most common laundering methods are: the purchase of high-value goods for cash; the use of credit institutions to receive and transfer funds in and out of Ireland; the use of complex company structures to filter funds; and the purchase of properties in Ireland and abroad. Ireland estimates that up to 80 percent of suspicious reports filed may involve tax violations.

The Government of Ireland (GOI) established the Shannon Free Zone in 1960 as a free trade zone offering investment incentives for multinational companies. The Shannon Free Zone is supervised by "Shannon Development," a government-founded body. Reportedly, there are no indications that criminals use the Shannon Free Zone in trade-based money laundering (TBML) schemes or by financiers of terrorism. The international banking and financial services sector is concentrated in Dublin's International Financial Services Centre (IFSC). In 2008, there were approximately 440 international financial institutions and companies operating in the IFSC. Services offered include banking, fiscal management, re-insurance, fund administration, and foreign exchange dealing. Although there are no tax benefits for companies in the IFSC, Ireland offers the lowest corporate tax rate (12.5 percent) in the EU. Casinos, including Internet casinos, are illegal in Ireland. Private gaming clubs, however, operate casino-like facilities that fall outside the scope of the law.

Ireland criminalized money laundering relating to narcotics trafficking and all indictable offenses under the 1994 Criminal Justice Act. The law requires financial institutions (banks, building societies, the Post Office, stock brokers, credit unions, bureaux de change, life insurance companies, and insurance brokers) to report suspicious transactions. There is no monetary threshold for reporting suspicious transactions. The obliged entities submit suspicious transaction reports (STRs) to the Garda (Irish Police) Bureau of Fraud Investigation, to Ireland's financial intelligence unit (FIU), and to the Revenue (Tax) Department, as required by law. Reporting entities must submit the STR before the suspicious transaction is finalized. There are no legal requirements governing the time period within which an STR must be filed. Financial institutions must implement customer identification procedures and retain records of financial transactions. Ireland has amended its Anti-Money Laundering (AML) law to extend customer identification and suspicious transaction reporting requirements to lawyers, accountants, auditors, real estate agents, auctioneers, and dealers in high-value goods. A conviction on charges of money laundering carries a maximum penalty of 14 years in prison and an unlimited fine. Ireland's Customer Due Diligence procedure requires designated entities to take measures to identify customers when opening new accounts or conducting transactions exceeding 13,000 euros ($17,000). These requirements do not extend to existing customers prior to May 1995 except in cases where authorities suspect that money laundering or another financial crime is involved.

The Corporate Law requires that every company applying for registration in Ireland must demonstrate that it intends to carry on an activity in the country. Companies must maintain an Irish resident director at all times or post a bond as a surety for failure to comply with the appropriate company law. In addition, the law limits the number of directorships that any one person can hold to 25, with certain exemptions. This limitation aims to curb the use of nominee directors as a means of disguising beneficial ownership or control. The Company Law Enforcement Act 2001 (Company Act) established the Office of the Director of Corporate Enforcement (ODCE). The ODCE investigates and enforces provisions of the Company Act. Under the law, a company must provide the names of its directors. The ODCE has the authority to uncover a company's beneficial ownership and control. The Company Act also creates a mandatory reporting obligation for auditors suspicious of breaches of company law to the ODCE. In 2007, the ODCE secured the conviction of 28 company directors and other individuals for breaching various requirements of the Company Act. An additional 14 company officers were disqualified from eligibility for a lead position in companies for periods ranging from one to 12 years.

Since June 15, 2007, Ireland has required travelers transporting more than 10,000 euros ($13,000) into or out of the EU to declare these funds. The declarations are automatically reported to the FIU. Customs authorities also require reports detailing movements of precious metals and stones into or out of the EU when Ireland is the initial entry or final exit point. The FIU has access to these reports as well. The ability to travel between Ireland and the U.K. without a passport poses a unique challenge for Irish law enforcement officials

As of November 2008, the European Commission had referred Ireland to the European Court of Justice for non-implementation of the Third EU Money Laundering Directive. The Government of Ireland (GOI) is likely to implement new legislation to address current shortcomings in customer due diligence, the identification of beneficial owners, politically exposed persons, and the designation of trusts. The Financial Action Task Force (FATF) conducted a mutual evaluation of Ireland in 2005. The mutual evaluation report (MER), published in 2006, acknowledged that although Ireland achieved a high standing in AML legal structures and international cooperation, the number of money laundering prosecutions and convictions was low.

The Irish Financial Services Regulatory Authority (IFSRA), the financial regulator, is a component of the Central Bank and Financial Services Authority of Ireland (CBFSAI) and is responsible for supervising the financial institutions for compliance with money laundering procedures. IFSRA is obliged to report any suspected breaches of the Criminal Justice Act 1994 by the institutions it supervises to the FIU and the Revenue Commissioners. Reports cover suspicion of money laundering and terrorist financing, failure to establish identity of customers, failure to retain evidence of identification, and failure to adopt measures to prevent and detect the commission of a money laundering offense. IFSRA also regulates the IFSC companies that conduct banking, insurance, and fund transactions.

Ireland's FIU receives and analyzes financial disclosures, and disseminates them for investigation. The MER found that although Ireland's FIU technically complied with the FATF Recommendations, it had limited technical and human resources to manage and evaluate STRs effectively. In 2007, the FIU received 11,145 STRs. Authorities convicted five people of money laundering and charged 11 others. Information regarding the number of STRs received in 2008 is not yet available. The lengthiest penalty applied for a money laundering conviction to date has been six years.

The Criminal Assets Bureau (CAB), authorized to confiscate the proceeds of crime in cases where there is no criminal conviction, reports to the Minister for Justice and includes experts from the Garda, Tax, Customs, and Social Security Agencies. Under the 1996 Proceeds of Crime Act, authorities may freeze specified property valued in excess of 13,000 euros ($17,000) for seven years, unless the court is satisfied that all or part of the property is not criminal proceeds. With the consent of the High Court

and the parties concerned, the authorities have the power to dispose of assets without having to wait the seven years. In 2007, the authorities executed 16 such consent orders. This Act also allows the authorities to take foreign criminality into account in assessing whether assets are the proceeds of criminal conduct. Under certain circumstances, the High Court can freeze, and, where appropriate, seize the proceeds of crimes.

In 2007, CAB obtained interim and disposal orders on assets valued at approximately 10.7 million euros ($14 million). The CAB has the authority to cooperate with agencies in other jurisdictions, strengthening Irish cooperation with asset recovery agencies in the United Kingdom.

With the Criminal Justice (Terrorism Offenses) Act, Ireland's legislation comports with United Nations Conventions. The IFSRA works with the Department of Finance to draft guidance for regulated institutions on combating and preventing terrorist financing. The authorities revised and issued guidance to institutions upon the passage of the Criminal Justice Act in 2005. To date, there have been no prosecutions for terrorism offenses under the Criminal Justice Act. The FATF MER noted that the Act neglects to criminalize funding of either a terrorist acting alone or two terrorists acting in concert. The MER also noted inadequate implementation of UN Security Council Resolution (UNSCR) 1373, in that Ireland relies exclusively on an EU listing system without subsidiary mechanisms to deal with terrorists on the list who are European citizens (EU Regulations do not apply for freezing purposes to such persons) or with persons designated as terrorists by other jurisdictions who are not on the EU list.

The Criminal Justice (Terrorism Offenses) Act imposes evidentiary requirements obstructing Ireland from fulfilling its UNSCR 1373 obligation to freeze all funds and assets of individuals who commit terrorist acts whether or not there is evidence that those particular funds are intended for use in terrorist acts. The Garda can apply to the courts to freeze assets when certain evidentiary requirements are met. From 2001 through 2008, Ireland had reported to the European Commission the names of five individuals who maintained a total of seven accounts that were frozen in accordance with the provisions of the European Union's (EU) Anti-Terrorist Legislation. No designated individuals or entities have surfaced in Ireland's system since 2004. The aggregate value of the funds frozen was $6,400.

A mutual legal assistance treaty (MLAT) between Ireland and the U.S. was signed in 2001. The United States and Ireland have also signed instruments to supplement and update that treaty as part of a sequence of bilateral agreements that the United States is concluding with all EU Member States. As of November 2008, the GOI had enacted legislation to bring the U.S.-EU MLAT and the U.S.-Ireland MLAT into force. Routine authorizations enabling notes to be exchanged still need to be executed; upon completion, the MLATs will enter fully into force.

Ireland is a member of the FATF, and its FIU is a member of the Egmont Group. Ireland is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the 1988 UN Drug Convention. It has signed, but not ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

The Government of Ireland should enact legislation to prohibit the establishment of "shell" companies and give law enforcement a stronger role in identifying the true beneficial owners of shell companies as well as of trusts in the course of investigations. Irish authorities should increase the technical and human resources provided to the FIU to manage and evaluate STRs effectively. Ireland should enact legislation that covers both funding of a terrorist acting alone and funding of two terrorists acting in concert, as well as legislation fully implementing UNSCR 1373. Ireland should ratify the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Isle of Man

Isle of Man (IOM) is a British crown dependency, and while it has its own parliament, government, and laws, the United Kingdom (UK) remains constitutionally responsible for its defense and international representation. Offshore banking, manufacturing, and tourism are key sectors of the economy. The government offers incentives to high-technology companies and financial institutions to locate on the island. Its large and sophisticated financial center is potentially vulnerable to money laundering at the layering and integration stages. Most of the illicit funds in the IOM are from fraud schemes and narcotics trafficking in other jurisdictions, including the UK. Identity theft and Internet abuse are growing segments of financial crime activity. The U.S. dollar is the most common currency used for criminal activity in the IOM.

As of December 31, 2008, there were 40 Banking, Building Society and Class 1 deposit taking license holders; 81 Investment Business and Class 2 investment business license holders; 61 Managers of Collective Investment Schemes and Class 3 services to collective investment schemes license holders; 204 Corporate Service Provider and Class 4 corporate services license holders; and 131 Trust Service Providers and Class 5 trust services license holders.

The IOM criminalized money laundering related to narcotics trafficking in 1987. The Criminal Justice (Money Laundering Offenses) Act 1998 extends the definition of money laundering to cover all serious crimes and leads to the creation of the Anti-Money Laundering Code, which came into force in December 1998. The Anti-Money Laundering Code was subsequently replaced by the Criminal Justice (Money Laundering) Code 2007, enacted in September 2007. In December 2008, the Criminal Justice (Money Laundering) Code 2008 (the Code) came into force. The Code revokes and replaces the Anti-Money Laundering Code 2007 and contains anti-money laundering (AML) provisions in line with the Financial Action Task Force's (FATF) Forty-Nine Recommendations.

The Code requires obligated entities to implement anti-money laundering/counterterrorist financing (AML/CTF) policies, procedures, and practices. The Code mandates that obligated entities institute procedures to establish customer identification requirements; report suspicious transactions; maintain adequate records; adopt adequate internal controls and communication procedures; provide appropriate training for employees; and establish internal reporting protocols. There is no minimum threshold for the filing of a suspicious transaction report (STR); and safe harbor provisions in the law protect reporting individuals when they file an STR. Failure to report suspicions of money laundering for all predicate crimes is a criminal offense. Failure to comply with the requirements of the Code may bring a fine, imprisonment of up to two years, or both.

The Financial Supervision Commission (FSC) and the Insurance and Pension Authority (IPA) regulate the IOM financial sector. The IPA regulates insurance companies, insurance management companies, general insurance intermediaries, and retirement benefit schemes and their administrators. The FSC is responsible for the licensing, authorization, and supervision of banks, building societies, investment businesses, collective investment schemes, corporate service providers, and companies. The FSC also maintains the Company Registry Database for the IOM, which contains company records dating back to 1865. Statutory documents filed by IOM companies can now be searched and purchased online through the FSC's website. In 2008, both the IPA and the FSC introduced revised regulations and guidance notes for their respective areas of supervision

The FSC has been undertaking a review of the AML/CTF regulations for its license holders as part of the Consolidation and Review of Regulatory Legislation (CAROL) Project. The output of CAROL has been a number of new acts and secondary legislation, which came into force on August 1, 2008. These changes revise the regulatory landscape for all financial services entities and activities regulated by the FSC, essentially all entities and activities other than those relating to insurance and pensions. The new Financial Services Rule Book 2008 details the requirements relating to AML/CTF with further guidance being found in the Anti-Money Laundering and Countering the Financing of Terrorism

Handbook. The main thrust of the Rule Book and Handbook has been to further develop the provisions relating to a risk-based approach to customer due diligence and to politically exposed persons (PEPs) in line with developments elsewhere around the globe.

The Insurance (Anti-Money Laundering) Regulations 2008 and the accompanying Guidance Notes on Anti-Money Laundering and Preventing of Terrorist Financing—for Insurers (Long Term Business) were produced by the IPA in the early part of 2008, and came into effect on September 1, 2008. The Regulations and Guidance Notes are derived from the previous Anti-Money Laundering Standards but also incorporate provisions relating to a more risk-based approach to customer due diligence and to dealing with PEPs.

The Isle of Man Law Society has produced the Guidance Notes 2008, which came into force on August 1, 2008. The Guidance Notes provide guidance to the legal profession on compliance with the Code. Following the implementation of the Code and the adoption of the Guidance Notes 2008, the position of advocates when they undertake relevant business is analogous to that applicable to solicitors in England and Wales.

Money service businesses (MSBs) not already regulated by the FSC or IPA must register with Customs and Excise. In December 2007, the FSC issued a Consultative Paper on the Proposed Regulation of MSBs, including electronic money (e-money) providers. This document assists the Island in meeting the standards set by the FATF Recommendations.

The Online Gambling Regulation Act 2001 and an accompanying AML (Online Gambling) Code 2002 are supplemented by AML guidance notes issued by the Gambling Supervision Commission (GSC), a regulatory body which provides guidance on the prevention of money laundering in the online gaming sector. The GSC was transferred from the Department of Home Affairs to the Treasury in 2007. In January, 2009, the Treasury is planning to introduce the new Gaming Control Bill to the Parliament. The Bill is primarily intended to make the GSC a Statutory Board, placing it on a level similar to the other regulatory bodies of the Treasury. The Bill also expands the constitution, status and authority of the GSC, and amends a number of minor issues that have arisen from application of the existing gaming legislative framework.

The Financial Services Act 2008 received Royal Assent in July 2008 and came into force on August 1, 2008. It was accompanied by consolidated secondary legislation and a new Rule Book. Transitional provisions allow existing license holders to continue carrying out regulated activities under their current licenses until January 1, 2009, at which time new licenses will be issued and the new Rule Book will fully apply. However, the new AML rules contained in the new Rule Book apply to all license holders beginning on August 1, 2008. The Act offers the Government ample flexibility to allow the regulations to be updated and improved in an ever changing economic environment. One of the significant improvements made to the regime provides for a new intermediate power to be granted to the FSC to formally warn a director or controller who is required to be fit and proper, but whose actions are questionable. This power would be appropriate where a formal sanction is warranted; stopping short of a "not fit and proper" direction, for example, where there is insufficient evidence to make such a direction. The Act also extends the FSC's powers in regard to investigation, inspection and power to require information, to include, in controlled circumstances, requests made by other regulators.

The new Act and Regulations have been the subjects of much consultation between the FSC and license holders, reflecting the Government's objective to ensure that any new rules are workable and represent a practical balance between regulatory constraints and the freedom required in order to promote business growth.

The Isle of Man's financial intelligence unit (FIU), the Financial Crime Unit (FCU), was formed in April 2000 under the Department of Home Affairs and evolved from the police Fraud Squad. The FIU

consists of personnel from Police and Customs with support personnel such as analysts and accountants provided by the Government Civil Service. The FCU is the national center for receiving, analyzing and disseminating STRs and other relevant intelligence. Annual statistics on STR information are published in the report of the Chief Constable of the Isle of Man. In 2006, the FIU received 1,651 STRs, down from 2,265 in 2005 and 2,315 in 2004. In 2007, the number continued to decline, to 1,561 STRs, 59 percent of which came from banks and an additional 21 percent from insurance service providers. The FCU has direct access on a real time basis to a wide range of intelligence databases, both nationally and internationally. Typologies and trends are fed back to the industry though lectures and presentations given by the FCU and in joint presentations and seminars with regulators.

IOM legislation provides powers to constables, including customs officers, to investigate whether a person has benefited from any criminal conduct. These powers allow information to be obtained about that person's financial affairs. These powers can be used to assist in criminal investigations abroad as well as in the IOM. The Customs and Excise (Amendment) Act 2001 gives various law enforcement and statutory bodies within the IOM the ability to exchange information, where such information would assist them in discharging their functions. The Act also permits Customs and Excise to release information it holds to any agency within or outside the IOM for the purposes of any criminal investigation and proceeding. Such exchanges can be either spontaneous or by request.

The new Proceeds of Crime Act 2008 came into force on October 1, 2008. The Act allows the recovery of property which is or represents property obtained through unlawful conduct, or which is intended to be used in unlawful conduct. It also provides for confiscation orders in relation to persons who benefit from criminal conduct and for restraint orders to prohibit dealing with property. Among others, the Act contains provisions concerning money laundering and the importation and exportation of cash; plus, provisions to give effect to overseas requests and orders related to property found or believed to be obtained through criminal conduct.

The Prevention of Terrorism Act 1990 makes it an offense to contribute to terrorist organizations or to assist a terrorist organization in the retention or control of terrorist funds. The IOM Terrorism (United Nations Measure) Order 2001 implements UNSCR 1373 by providing for the freezing of terrorist funds, as well as by criminalizing the facilitating or financing of terrorism. The Government of the IOM enacted the Anti-Terrorism and Crime Act, 2003, which makes the failure to report suspicious transactions relating to money intended to finance terrorism an offense. All other UN and European Union financial sanctions have been adopted or applied in the IOM, and are administered by Customs and Excise. Institutions are obliged to freeze affected funds and report the facts to Customs and Excise.

All charities operating within the IOM are registered and supervised by the Charities Commission. In May 2008, the Chief Secretary's Office published a consultation paper, "Charities and other Non-Profit Organizations," which was an invitation to comment on options for the registration, regulation and monitoring of such bodies to prevent their possible use in the financing of terrorism. There is no suggestion that nonprofit organizations in the Isle of Man are being used for such purposes. The IOM government reviewed the regulation of this type of organization to ensure the Island's system is not vulnerable to abuse in future by international elements.

In 2008, the International Monetary Fund (IMF) examined the regulation and supervision of the IOM's financial sector. This represented the most comprehensive review of the Island's regulatory and AML/CTF framework to date. The results of the assessment are due to be published in 2009.

The FSC continues to work with the Crown Dependencies Guernsey and Jersey to develop a coordinated strategy on money laundering, and to ensure maximum compliance with the FATF Recommendations.

Although not a member of the FATF, the Island fully endorses the FATF Recommendations. The IOM's experts are assisting the FATF working group that considers matters relating to customer identification and companies' issues. The IOM is a member of the Offshore Group of Banking Supervisors (OGBS) and Offshore Group of Insurance Supervisors (OGIS). The FCU is a member of the Egmont Group.

The IOM cooperates with international AML authorities on regulatory and criminal matters. Under the 1990 Criminal Justice Act, the provision of documents and information is available to all countries and territories for the purposes of investigations into serious or complex fraud, drug-trafficking and terrorist investigations. All decisions for assistance are made by the Attorney General of the IOM on a case-by-case basis, depending on the circumstances of the inquiry.

As part of its continuing program of developing closer economic and taxation co-operation with other countries, the Isle of Man concluded agreements with the Government of Australia on January 29, 2009. The two agreements are: a tax information exchange agreement based on the Organization for Economic Co-operation and Development (OECD) model; and an agreement addressing the allocation of taxing rights over certain income of individuals and the establishment of a mutual agreement procedure in respect to transfer pricing adjustments. Previously, the IOM signed tax information exchange agreements (TIEAs) with each member of the Nordic Council and the United States, where it has established protocols with the Internal Revenue Service (IRS) to ensure that information exchange requests are handled smoothly.

Application of the 1988 UN Drug Convention was extended to the IOM in 1993. In 2003, the U.S. and the UK agreed to extend to the Isle of Man the U.S.-UK Treaty on Mutual Legal Assistance in Criminal Matters.

The Isle of Man has had AML/CTF legislation in place for well over a decade. The new regulatory regime consolidates and simplifies the old regime and provides a transparent and user-friendly regulatory environment, further promoting the Isle of Man as a leading offshore market. The IOM should act on the 2007 Consultative paper containing the MSB/e-money regulation proposals and implement those most effective. Isle of Man officials should continue to support and educate the local financial sector to help it combat current trends in money laundering and terrorist financing. The IOM should ensure that obliged entities understand and respond to their new and revised responsibilities. The authorities also should continue to work with international AML/CTF authorities to deter financial crime and the financing of terrorism and terrorists.

Israel

Israel has a high GDP, per capita income, developed financial markets and diverse capital markets. Nevertheless, Israel is not regarded as a regional financial center. It primarily conducts financial activity with the markets of the United States and Europe, and to a lesser extent with the Far East. There has been no significant change in the Israeli anti-money laundering and combating of terrorism financing (AML/CTF) law for 2008 and the Israeli National Police (INP) reports no indication of an increase in financial crime relative to previous years. A 2008 report by MONEYVAL, a FATF-style regional body, states that the overall threat of money laundering and terrorist financing in Israel is "considerable," with more than $5 billion in illicit proceeds generated through illegal drugs, gambling, extortion, fraud, and human trafficking. Criminal groups in Israel with ties to the former Soviet Union, United States, and European Union often utilize a maze of offshore shell companies and bearer shares to obscure beneficial owners. Recent studies conducted by the INP Research Department estimate illegal gambling profits at over $2 billion per year and domestic narcotics profits at $1.5 billion per year. Human trafficking is considered the crime-for-profit with the greatest human toll in Israel, and public corruption the crime with the greatest social toll. As such, these areas are the targets of the most vigorous anti-money laundering enforcement activity. Black market penetration in Israel remains low

and is comparable in scale to that of western, industrialized nations. While there have been some reports of trade-based money laundering, Israeli enforcement capacity is adequate to keep the problem to minimum levels. With the exception of a few isolated incidents involving the sales of drugs in the United States by Israeli organized crime, Israel's illicit drug trade is domestically focused and has little to no connection with illegal drug sales in the United States. Israel does not have free trade zones and is not considered an offshore financial center, as offshore banks and other forms of exempt or shell companies are not permitted. Bearer shares, however, are permitted for banks and/or for companies.

In August 2000, Israel enacted its anti-money laundering legislation, the Prohibition on Money Laundering Law (PMLL, Law No. 5760-2000). The PMLL established a framework for an AML system, but required the passage of several implementing regulations before the law could fully take effect. Among other things, the PMLL criminalized money laundering and included 18 serious crimes, in addition to offenses described in the prevention of terrorism ordinance, as predicate offenses for money laundering even if committed in a foreign jurisdiction.

The PMLL also provided for the establishment of the Israeli Money Laundering Prohibition Authority (IMPA) under the Ministry of Justice, as the country's financial intelligence unit (FIU). IMPA became operational in 2002. The PMLL requires financial institutions to report "unusual transactions" to IMPA as soon as possible. Financial institutions must report all transactions that exceed a minimum threshold that varies based on the relevant sectors and the risks that may arise, with more stringent requirements for transactions originating in a high-risk country or territory. IMPA has access to population registration databases, the Real-Estate Database, records of inspections at border crossings, court files, and Israel's Registrar of Companies.

In 2001, Israel adopted the Banking Corporations Requirement Regarding Identification, Reporting, and Record Keeping Order. The Order establishes specific procedures for banks with respect to customer identification, record keeping, and the reporting of irregular and suspicious transactions in keeping with the recommendations of the Basel Committee on Banking Supervision. The Supervisor of Banks at the Bank of Israel monitors compliance among banking institutions. Bankers and others are protected by law with respect to their cooperation with law enforcement entities.

Subsequent regulations established methods of reporting to the Customs Authority (an agency of the Israel Tax Authority) monies brought in or out of Israel, and criteria for financial sanctions for violating the law, as well as for appeals. The regulations require the declaration of currency transferred (including cash, travelers' checks, and banker checks) into or out of Israel for sums above 80,000 new Israeli shekels (NIS) (approximately $20,500). This applies to any person entering or leaving Israel, and to any person bringing or taking money into or out of Israel by mail or any other methods, including cash couriers. Failure to comply is punishable by up to six months imprisonment or a fine of NIS 202,000 (approximately $52,000), or ten times the amount that was not declared, whichever is higher. Alternatively, an administrative sanction of NIS 101,000 (approximately $26,000), or five times the amount that was not declared, may be imposed by the Committee for Imposition of Financial Sanctions. In May 2008, Agents from U.S. Immigration and Customs Enforcement (ICE) and officers from U.S. Customs and Border Protection (CBP) conducted joint bulk currency interdiction operations with Israeli law enforcement counterparts in Israel and at U.S. airports as part of the Department of Homeland Security's (DHS) "Hands Across the World" initiative. The coordinated law enforcement effort resulted in an arrest and two seizures in the United States and 14 seizures in Israel. The combined seizures totaled nearly $500,000 in cash, negotiable checks, gold and diamonds. In 2003, the Government of Israel (GOI) lowered the threshold for reporting cash transaction reports (CTRs) to NIS 50,000 (approximately $12,800), lowered the document retention threshold to NIS 10,000 (approximately $2,570), and imposed more stringent reporting requirements.

Clarifications to the PMLL were approved in Orders 5761-2001 and 5762-2002 requiring that suspicious transactions be reported by members of the stock exchange, portfolio managers, insurers or

insurance agents, provident funds and companies managing a provident fund, providers of currency services, and the Postal Bank. Portfolio managers and members of the stock exchange are supervised by the Chairman of the Israel Securities Authority; insurers and insurance agents are under the authority of the Superintendent of Insurance in the Ministry of Finance; provident funds and companies managed by a provident fund are overseen by the Commissioner of the Capital Market in the Ministry of Finance, and the Postal Bank is monitored by the Minister of Communications.

Other subsequent changes to the PMLL authorized the issuance of regulations requiring financial service providers to identify, report, and keep records for specified transactions for seven years; the establishment of a mechanism for customs officials to input into the IMPA database; the creation of regulations stipulating the time and method of bank reporting; the creation of rules on safeguarding the IMPA database; and rules for requesting and transmitting information between IMPA, the INP and the Israel Security Agency (ISA, or Shin Bet). The PMLL also imposed an obligation on financial service providers to report any IMPA activities perceived as unusual.

Order 5762 added money services businesses (MSB) to the list of entities required to file cash transaction reports (CTRs) and suspicious transaction reports (STRs) by size and type, and required that they preserve transaction records for at least seven years. The PMLL mandates the registration of MSBs through the Providers of Currency Services Registrar at the Ministry of Finance. A person engaging in the provision of currency services without being registered is liable to one year of imprisonment or a fine of NIS 600,000 (approximately $154,000). According to MONEVAL, there are exemptions that allow intermediaries such as accountants, attorneys and rabbis to not disclose who their clients are if transactions are less than the equivalent of $69,000 in one day.

On July 11, 2007 a draft bill for PMLL (Amendment No. 7) 5776-2007 was published for the purpose of extending Israel's AML regime to the trade in precious stones (including Israel's substantial diamond trading industry). The bill passed the first vote in the Knesset on August 16, 2007 and was submitted to committee for review. Having been approved by the Constitution, Law and Justice Committee, the bill is ready to be brought again before the plenum of the Knesset (legislative body) for the second and third readings. If it passes it will bring the AML regime within the precious stones sector in line with international standards. The amendment defines "dealers in precious stones" as those merchants whose annual transactions reach NIS 50,000 (approximately $12,800). It places significant obligations on dealers to verify the identity of their clients, report all transactions above a designated threshold (and all unusual client activity) to IMPA, as well as to maintain all transaction records and client identification for at least five years. The Customs Authority continues to intercept unreported diamond shipments, despite the fact that Israel imposes no tariffs on diamond imports.

In December 2004, the Israeli Parliament adopted the prohibition on terrorist financing law 5765-2004, which further modernized and enhanced Israel's ability to combat terrorist financing and to cooperate with other countries on such matters. The Law went into effect in August 2005, criminalizing the financing of terrorism as required by United Nations Security Council Resolution (UNSCR) 1373. The Israeli legislative regime criminalizing the financing of terrorism includes provisions of the Defense Regulations State of Emergency/1945, the Prevention of Terrorism Ordinance/1948, the Penal Law/1977, and the PMLL. Under the International Legal Assistance Law of 1998, Israeli courts are empowered to enforce forfeiture orders executed in foreign courts for crimes committed outside Israel.

In October 2006, the Knesset Committee on Constitution, Law and Justice approved an amendment to the Banking Order and the Regulations on the Prohibition on Financing Terrorism. The Order and Regulations were additional steps in the legislation intended to combat the financing of terrorism while maintaining correspondent and other types of banking relationships between Israeli and Palestinian commercial banks. Although the amendment to the Order and the Regulations impose serious obligations on banks to examine clients and file transaction reports, banks are still exempted

from criminal liability if, *inter alia*, they fulfill all of their obligations under the Order (though they are not protected from civil liability). The Banking Order was expanded to cover the prohibition on financing terrorism and includes obligations to check the identification of parties to a transaction against declared terrorists and terrorist organizations, as well as obligations to report by size and type of transaction. The Banking Order sets the minimum size of a transaction that must be reported at NIS 5,000 (approximately $1,280) for transactions with a high-risk country or territory. The order also includes examples for unusual financial activity suspected to be related to terrorism, such as transfers from countries with no anti-money laundering or counterterrorist finance (AML/CTF) regime to nonprofit organizations (NGOs) within Israel and the occupied territories. Banks are required to file suspicious transaction reports with the IMPA and their adherence to the Banking Order is adequately regulated by the Banking Supervision Department at the Bank of Israel, the Central Bank. The Bank of Israel is adequately staffed and trained and has fined Israeli commercial banks in the past for failing to report suspicious data as required by law.

In October 2006, the U.S. Department of Treasury, the Federal Deposit Insurance Corporation, and the New York State Banking Department penalized Israel Discount Bank $12 million to settle charges that its AML procedures were lax. The action was specifically related to the transfer of billions of dollars of illicit funds from Brazil to Israel Discount Bank's New York offices. In December, 2008 the Bank of Israel also ordered that Israel Discount Bank pay nearly $1 million in fines over the institution's poor money laundering controls.

In 2008, Israel finished implementing all but one mandate of Cabinet Decision 4618, passed on January 1, 2006. Yet to be established is an academy for interdisciplinary enforcement studies; however, an interagency "fusion center" and six interagency task forces for pursuing financial crimes are now fully operational. The regulation explicitly instructs the INP and the Israeli Security Agency, known as Shin Bet to target illicit proceeds as a primary objective in the war on organized crime. As Israel does not have legislation preventing financial service companies from disclosing client and ownership information to bank supervisors and law enforcement authorities, the new regulation establishes conditions for the use of such information to avoid its abuse and to set guidelines for the police and security services.

Israel has established systems for identifying, tracing, freezing, seizing, and forfeiting narcotics-related assets, as well as assets derived from or intended for other serious crimes, including the funding of terrorism and trafficking in persons. The law also allows for civil forfeiture when ordered by the District Court. The identification and tracing of such assets is part of the ongoing function of the Israeli intelligence authorities and IMPA. The INP has responsibility for seizing assets and the State Attorney's Office has authority to freeze assets. Banking institutions cooperate fully, and often freeze suspicious assets according to guidance from the INP and Ministry of Defense. Israel's International Legal Assistance Law enables Israel to offer full and effective cooperation to authorities in foreign states, including enforcement of foreign forfeiture orders in terror financing cases (both civil and criminal). The IMPA reports that about NIS 4.6 million ($1.2 million) was forfeited or collected in penalties related to illicit narcotics-related actions.

In December 2007, the Knesset Law Committee approved new regulations enabling the declaration by a ministerial committee of foreign designated terrorists, and legally requiring financial institutions to comply with the foreign designations. The committee instructed the Israeli National Security Council (NSC) to develop a procedure to incorporate foreign designations into Israel's regime for domestic designations. In this new procedure, the National Security Council legal counsel has responsibility for referring foreign designations to the committee for adoption under Israeli law. As of late 2008, the procedure remains under review for final approval by all of the Israeli Security Services. After vetting through these agencies, the NSC will submit the procedure to the Knesset Law Committee for final approval. Once in effect, the NSC is expected to include entities on the UNSCR 1267 Sanctions Committee consolidated list and entities on the list of Specially Designated Global Terrorists

designated by the United States pursuant to E.O. 13224. Thereafter identifying information for the terrorist entity will be published on the Ministry of Defense website, in two daily newspapers, the Official Gazette of the Israeli Government, and distributed by email to financial institutions. Israel already enforces UNSCR 1267 under its Trade with the Enemy Ordinance of 1939, and regularly notifies financial institutions of restricted entities.

The Shin Bet is responsible for investigating terrorist financing offenses, while the Israel Tax Authority handles investigations originating in customs offenses. Under Israeli law, it is a felony to conceal cash transfers upon entry to the West Bank or Gaza, and the agencies coordinate closely to track funds that enter Israeli ports. Customs and the Ministry of Defense also cooperate in combating trade-based terrorist financing, including goods destined for terrorist entities in the West Bank or Gaza.

Through regulation of the Ministry of Finance, the PMLL prohibits any unlicensed money changers or providers of currency services. Among other definitions, the PMLL defines a provider of currency as one who receives financial assets in one state in exchange for making available financial assets in another state. This definition has broad scope and therefore restricts hawala, hundi, or alternative remittance systems. A person engaging in provision of currency services without proper registration is liable to one year imprisonment or a fine of NIS 600,000 (approximately $154,300). Israel's Law of Non-Profit Organizations allows for the creation of "Public Welfare" organizations, known as amitot in Hebrew. Israel acknowledges that these entities can be used as conduits for the financing of terrorism or other illicit activity and therefore it rigorously regulates the sector. The Registrar of Trusts is charged with oversight of amitot and maintains the power to demand clarification of financial statements, investigation, closure and can petition the court to liquidate such organizations that it believes violate the law. Furthermore, the Registrar of Trusts is empowered to turn over such information as it deems appropriate to enable law-enforcement to conduct criminal investigations. The IMPA reports that approximately 700 extensive audits of high-income amitot are carried out annually.

The INP and the Financial Service Providers Regulatory Authority maintain a high level of coordination, routinely exchange information, and have conducted multiple joint enforcement actions. The INP reports no indications of an overall increase in financial crime relative to previous years. Total criminal assets seized by the INP in 2008 were reportedly $3.2 million. This is a sharp decrease from previous years. In 2008, IMPA reported approximately 100 arrests and ten prosecutions relating to money laundering and/or terrorist financing. In 2008, IMPA received 17,152 suspicious transaction reports. During this period IMPA disseminated 529 intelligence reports to law enforcement agencies and to foreign FIUs. For 2008, the IMPA reports that about NIS 7.7 million ($2 million) was frozen or forfeited in AML/CTF-related actions

Israel has a Mutual Legal Assistance Treaty with the United States, as well as a bilateral mutual assistance agreement in customs matters. Customs, IMPA, the INP and the Israel Securities Agencies routinely exchange information with U.S. agencies through their regional liaison offices, as well as through the Israel Police Liaison Office in Washington. Israel provides assistance in sharing information related to terrorist financing cases.

Israel is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. Israel has signed but not yet ratified the UN Convention against Corruption. The IMPA is a member of the Egmont Group, and Israel has been an active observer in MONEYVAL since 2006. Israel is the only nonmember of the Council of Europe to become a party to the European Convention on Mutual Assistance in Criminal Matters (in 1967) and its Second Additional Protocol (in 2006), which is designed to provide more effective and modern means of assisting member states in law enforcement matters.

The Government of Israel has developed an AML/CTF financial regulatory sector and enforcement capacity that compares with advanced, industrialized nations. Israel remains deficient, however, in regulating its diamond trade, intermediaries such as accountants and lawyers, other nonbank sectors, and fully incorporating UNSC 1267 designations into its domestic regime due primarily to political uncertainty in the Knesset, which have prevented timely implementation. Authorities should be vigilant in ensuring draft legislation and proposed measures are approved by final act of the Knesset following the establishment of a new government in 2009. Israel should continue its aggressive investigation of money laundering activity associated with organized criminal groups. Israel should ratify the UN Convention against Corruption.

Italy

Italy is not an offshore financial center. Italy is part of the Euro area and is fully integrated into the European Union (EU) single market for financial services. Money laundering is a concern because of the prevalence of homegrown organized crime groups as well as criminal organizations from abroad, especially from Albania, Bulgaria, China, Israel, Romania and Russia.

The heavy involvement of organized crime groups in narcotics-trafficking complicates narcotics-related anti-money laundering (AML) activities because of the sophistication of the laundering methods used by these groups. Italy is both a consumer country and a major transit point for heroin coming from South Asia through the Balkans en route to Western/Central Europe and, to a lesser extent, the United States. Italian and ethnic Albanian criminal organizations work together to funnel drugs to Italy and, in many cases, on to third countries. Additional important trafficking groups include other Balkan organized crime entities, as well as Nigerian, Colombian, and other South American trafficking groups.

In addition to the narcotics trade, laundered money originates from myriad criminal activities, such as alien smuggling, contraband cigarette smuggling, counterfeit goods, extortion, human trafficking, and usury. Financial crimes not directly linked to money laundering, such as credit card fraud, Internet fraud, and phishing have increased over the past year.

Money laundering occurs both in the regular banking sector and in the nonbank financial system, including casinos, money transfer houses, and the gold market. Money launderers predominantly use nonbank financial institutions for the export of undeclared or illicitly obtained currency—primarily U.S. dollars and euros—for laundering in offshore companies. There is a substantial black market for smuggled goods in the country, but it is not believed to be funded significantly by narcotics proceeds. Italy's underground economy is an estimated 20-27 percent of Italian GDP, totaling about 309 to 417 billion euros (approximately $417,150,000,000 to $562,950,000,000), though a substantial fraction of this total is related to tax evasion of otherwise legitimate commerce.

Legislative decree 109 of 2007 provides for the permanent establishment of the Financial Security Committee (FSC), originally created in 2001. The FSC's activities include prevention of money laundering and terrorist financing, and implementing international economic sanctions. The Committee is chaired by the Director General of the Treasury. Other FSC members include the Ministries of Foreign Affairs, Home Affairs, and Justice; the Bank of Italy; the Unita' di Informazione Finanziaria (UIF), Italy's financial intelligence unit (FIU); CONSOB, Italy's securities market regulator; the Guardia di Finanza or Financial Police (GdF); the Carabinieri (paramilitary police); the National Anti-Mafia Directorate (DNA); and the Anti-mafia Administration or Direzione Investigativa Antimafia (DIA). The Committee has far-reaching powers that include waiving provisions of the Official Secrecy Act to obtain information from all government ministries. Legislative decree 109 also empowers the FSC to submit proposals to the competent UN or EU authorities on the listing or de-listing of individuals or entities subject to restrictions on financial transactions and/or asset freezes.

Italy's anti-money laundering and counterterrorist financing (AML/CTF) regime is comprehensive. Money laundering is defined as a criminal offense when laundering relates to a separate, intentional felony offense. All intentional criminal offenses are predicates to the crime of money laundering, regardless of the applicable sentence for the predicate offense. It should be noted that Italian law does not allow someone to be prosecuted for laundering the proceeds of crimes they themselves committed. This reflects Italian concern with possible double jeopardy. In other words, a person can only be prosecuted for laundering the proceeds of crimes committed by other persons. The law protects bankers and others with respect to their cooperation with law enforcement entities.

Legislative decree 231 of 2007 broadens the range of predicate offenses for money laundering and requires covered entities to report self-money laundering to the UIF through STRs. The decree also enhances penalties for the transfer of property when the subject knows the property was derived from criminal activity, as well as the concealment or disguise of the true origin of any property.

The Ministry of Economy and Finance is in charge of general policy making and coordination in the AML/CTF arena. It also has sanctioning powers related to specific AML requirements (e.g., record keeping requirements and cash transaction limitations). In 2007, 1,676 administrative proceedings were settled by ministerial decrees, resulting in fines and penalties of 16.4 million euros (approximately $22,140,000). Since the introduction of AML laws in 1991, approximately 27,880 administrative proceedings have been settled, with sanctions imposed to date totaling about 98 million euros (approximately $132,300,000).

Italy has strict laws on the control of currency deposits in banks. Banks must identify their customers and record any transaction that exceeds 15,000 euros (approximately $20,250). Bank of Italy mandatory guidelines require the reporting of all suspicious transactions, with special attention paid to cash anomalies. Italian law prohibits the use of cash or negotiable bearer instruments for transferring money in amounts in excess of 12,500 euros (approximately $16,900), except in transactions performed by banks, e-money institutions (which issue electronic money over the Internet for e-commerce) and the postal service.

Legislative decree 231 of 2007 reviews the customer due diligence (CDD) requirements, following a risk-based approach, and indicates those cases where enhanced or simplified CDD applies. Obliged entities now must obtain senior management approval before establishing a business relationship with a politically exposed person (PEP) and must take adequate measures to establish the source of funds involved in any transaction with a PEP. Legislative Decree 231 introduces the notion of a beneficial owner, which refers to the natural person who ultimately owns or controls an account and/or the person on whose behalf a transaction is being conducted. It also includes those persons who exercise effective control over a legal person or arrangement. Banks and other financial institutions must identify the beneficial owners of accounts they open and be able to track the transactions they conduct. Anonymous accounts are prohibited, as are bearer passbooks with a balance exceeding 12,500 euros (approximately $16,900). Italy prohibits financial institutions from entering into correspondent banking relationships with shell banks or with a bank known to permit its accounts to be used by a shell bank.

Banks and other financial institutions are required to maintain records necessary to reconstruct significant transactions for ten years. This includes information about the point of origin of funds transfers and related messages sent to or from Italy. Banks operating in Italy must record account data in standardized customer databases. A "banker negligence" law makes individual bankers responsible if their institutions launder money. The legal responsibility to submit STRs is not exclusive to bankers, though the Italian judiciary metes out more severe punishment to bankers for noncompliance. Financial institutions are required to maintain a centralized electronic AML database for all transactions (including wire transfers) over 15,000 euros (approximately $20,250) and to submit this

data monthly to the UIF. The data is aggregated by class of transaction, and any reference to customers is removed. The UIF analyzes the data and can request specific transaction details if warranted.

To deter nontraditional money laundering, the Government of Italy (GOI) enacted a decree in 2004 to broaden the category of institutions and professionals subject to AML regulations. The list now includes accountants, debt collectors, exchange houses, insurance companies, casinos, real estate agents, brokerage firms, gold and valuables dealers and importers, auction houses, art galleries, antiques dealers, labor advisors, lawyers, and notaries. The necessary implementing regulations for the designated nonbank financial businesses and professions (DNFBPs) came into force in April 2006 (Ministerial Decrees no. 141, 142 and 143 of 3.02.2006). Italy now has comprehensive internal auditing and training requirements for its broadly-defined financial sector. However, implementation of AML/CTF measures by nonbank financial institutions lags behind that of financial institutions, as evidenced by the continuing relatively low number of STRs filed by DNFBPs. The issue of client confidentiality for attorneys remains unresolved so compliance with AML/CTF provisions is uneven in that sector.

Italy has addressed the problem of international transportation of illegal-source currency and monetary instruments by applying the 10,000 euro-equivalent (approximately $13,500) reporting requirement to cross-border transport of domestic and foreign currencies and negotiable bearer instruments. Italy has a declaration system, rather than disclosure, and the fines for failure to declare a cross-border transaction or transport of funds may be up to 40 percent of the amount beyond the threshold.

Responsibility for ensuring compliance with AML/CTF varies by sector. The Bank of Italy supervises banks both on-site and off-site, as well as nonbank financial intermediaries. The Ministry of Justice exercises general oversight of some DNFBPs (e.g., attorneys, accountants, and notaries) though day-to-day supervision is provided by professional organizations. The Ministry of Interior is responsible for other nonfinancial businesses and professions (e.g., casinos, entities engaged in the custody and transportation of cash and other valuables, real estate agents, and collection agencies). ISVAP (Institute for Insurance Industry Oversight) monitors the insurance industry. In 2007, ISVAP performed 19 inspections of insurance entities, an increase of 72 percent over the previous year. In May 2008, the Bank of Italy conducted its first cycle of on-site AML inspections of bank branches located in high risk areas. The Bank of Italy completed 319 such inspections through October of 2008, and plans to expand the program nationwide in 2009.

On January 1, 2008, the UIF replaced the Ufficio Italiano dei Cambi (UIC) as Italy's FIU. The UIF is an autonomous entity within the Bank of Italy with approximately 90 employees. The UIF performs advisory functions on AML/CTF legislation. It also proposes and updates indicators of anomalous activity and analyzes financial information. The UIF has access to the banks' customer databases and does not require a court order to compel supervised institutions to provide details on regulated transactions. It submits its financial analyses on STRs to law enforcement agencies, including the DIA and GdF, for further investigation and/or prosecution. The UIF received 11,994 STRs in 2007 from credit and financial institutions, and 6,664 in the first half of 2008. In 2007 the UIF sent 11,513 money laundering reports to law enforcement authorities for further investigation. Through the first half of 2008 the equivalent figure was 5,823. STRs resulted in 217 cases of judicial follow up in 2007, and 56 cases in the first half of 2008. The UIF received only 216 STRs from DNFBPs in 2007, and 54 through June 2008. In 2007, the FIU received 335 STRs related to terrorist financing, of which 211 were forwarded to law enforcement for further investigation. Through June 30, 2008, the UIF had received 146 terrorist financing-related STRs. The UIF may provisionally suspend for five days suspected money laundering or terrorist financing transactions, rather than the 48 hour period to which the UIC was restricted.

A special currency branch of the GdF is the law enforcement agency with primary jurisdiction for conducting financial investigations. Investigators from the GdF and other law enforcement agencies

must obtain a court order prior to being granted access to bank records or databases. In 2007, the GdF carried out 341 AML inspections, which resulted in 47 administrative violations, as well as 362 criminal violations and 618 legally reported subjects (analogous to being advised one is the target of an investigation). In 2007, there were also 1,225 AML/CTF inspections related to money transfers, which resulted in 866 legally reported subjects and 14 arrests.

Italy has established reliable systems for identifying, tracing, freezing, seizing, and forfeiting assets from narcotics-trafficking and other serious crimes, including terrorism. These assets include currency accounts, real estate, vehicles, vessels, drugs, legitimate businesses used to launder drug money, and other instruments of crime. Under anti-mafia legislation, seized financial and nonfinancial assets of organized crime groups can be forfeited. Italy does not have any significant legal loopholes that allow traffickers and other criminals to shield assets. However, the burden of proof is on the Italian government to make a case in court that assets are related to narcotics-trafficking or other serious crimes. Law enforcement officials have adequate powers and resources to trace and seize assets, with judicial concurrence. Funds from asset forfeitures are entered into the general state accounts. Italy shares assets with member states of the Council of Europe. Currently, assets can be shared bilaterally only if agreement is reached on a case-specific basis. Legislative decree 109 of 2007 gives the Agenzia del Demanio (State Property Agency) the responsibility to manage frozen terrorist-related assets, in addition to its previous responsibility for sequestered criminal assets.

The financing of terrorist activity has been a criminal offense since 2001, with prison terms of between seven and 15 years. Financial institutions, including DNFBPs, are required to report suspicious activity related to terrorist financing. Italy currently has frozen $6,238,186 in assets in 29 accounts, belonging to persons designated terrorists under UNSCRs 1333, 1390 and 1373. The GOI cooperates fully with efforts by the United States to trace and seize assets. The UIF disseminates the EU, UN, and U.S. Government lists of terrorist groups and individuals to financial institutions. Following the UIF's provisional suspension for five days of suspected money laundering or terrorist financing transactions, the courts must act to freeze or seize the assets. Under Italian law and EU regulation, financial and economic assets linked to terrorists designated by the EU can be directly frozen by the financial intermediary holding them. Assets can be seized through a criminal sequestration order.

Italy does not regulate charities per se. Primarily for tax purposes, in 1997, Italy created a category of "not-for-profit organizations of social utility" (ONLUS). Such organizations can be associations, foundations or fundraising committees. To be classified as an ONLUS, the organization must register with the Finance Ministry and prepare an annual report. There are currently 19,000 registered entities in the ONLUS category. Established in 2000, the ONLUS Agency issues guidelines and drafts legislation for the nonprofit sector, alerts other authorities of violations of existing obligations, and confirms de-listings from the ONLUS registry. The ONLUS Agency cooperates with the Finance Ministry in reviewing the ONLUS classification conditions. The ONLUS Agency has reviewed 1,500 entities and recommended the dissolution of several that were not in compliance with Italian law. Italian authorities believe there is a low risk of terrorist financing in the Italian nonprofit sector.

In Italy, the term "alternative remittance system" refers to regulated nonbank institutions such as money transfer businesses. Informal remittance systems do exist, primarily to serve Italy's significant immigrant communities, and in some cases, they are used by Italy-based drug-trafficking organizations to transfer narcotics proceeds.

As a member of the Egmont Group, Italy's UIF shares information on suspicious financial transactions with other countries' FIUs. To date Italy has never refused a request for assistance in providing information to another nation's FIU. In 2007, Italy responded to 448 requests for information from foreign FIUs, resulting in 990 reported persons. Italy has a number of bilateral agreements with foreign governments in the areas of investigative cooperation on narcotics-trafficking and organized

crime. The United States and Italy have signed a customs assistance agreement, as well as extradition and mutual legal assistance treaties. Both in response to requests under the mutual legal assistance treaty (MLAT) and on an informal basis, Italy provides the United States records related to narcotics-trafficking, terrorism and terrorist financing investigations and proceedings. Italy also cooperates closely with U.S. law enforcement agencies and other governments investigating illicit financing related to these and other serious crimes. In May 2006, the U.S. and GOI signed a new bilateral instrument on mutual legal assistance as part of the process of implementing the U.S.-EU Agreement on Mutual Legal Assistance, signed in June 2003. Once ratified and brought into force, the new U.S./Italy bilateral treaty will allow for greater mutual assistance in the seizure and forfeiture of assets as well as the sharing of those forfeited assets. As of November 2008, Italy has not ratified this treaty.

Italy is a member of the Financial Action Task Force (FATF) and held the FATF presidency from 1997 to 1998. Italy is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, and UN Convention against Transnational Organized Crime. Italy has signed, but not yet ratified, the UN Convention against Corruption.

The Government of Italy appears committed to the fight against money laundering and terrorist financing, both domestically and internationally. Given the relatively low number of STRs being filed by nonbank financial institutions, the GOI should improve its training efforts and supervision in this sector and should clarify attorney/client privilege. Italy should take steps to allow for civil in rem forfeiture of criminal proceeds. Italy should add car dealerships to the list of entities required to submit STRs, as they are notably absent. Italian law enforcement agencies should take additional steps to understand and identify underground finance and value transfer methodologies employed by Italy's burgeoning immigrant communities. Italy also should ensure its new regulations on PEPs are enforced, to prevent money laundering and counter corruption. The GOI should ratify both the UN Convention against Corruption and the bilateral instrument on Mutual Legal Assistance. Finally, Italy should continue its active participation in multilateral fora dedicated to the global fight against money laundering and terrorist financing and its assistance to jurisdictions with nascent or developing AML/CTF regimes.

Jamaica

Jamaica is the foremost producer and exporter of marijuana in the Caribbean, and an active transit route for cocaine flowing from South America to the United States and other international destinations. In addition to profits from domestic marijuana trafficking, payments for cocaine and weapons pass through Jamaica in the form of bulk cash shipments back to South America. The majority of funds being laundered in Jamaica are from drug traffickers and organized crime groups, which need to legitimize both profits from overseas criminal activity as well as domestic fraud and extortion schemes. Proceeds from drug trafficking and other criminal activity are used to acquire tangible assets and are moved back into legitimate markets through unregulated investments and hidden in remittance flows. Public corruption, particularly in the Customs Service, provides opportunities for trade- based money laundering. The Government of Jamaica (GOJ) continues to advance its plans to turn Kingston into an offshore financial center, and to license high-end casino gaming. If actuated Jamaica's vulnerability to money laundering will markedly increase.

To date, Jamaica has not been considered a major money laundering country. Jamaican banking authorities currently do not license offshore banks or other forms of exempt or shell companies, nor are nominee or anonymous directors and trustees allowed for companies registered in Jamaica. Financial institutions are prohibited from maintaining anonymous, numbered or fictitious accounts under the 2007 Proceeds of Crime Act. The GOJ does not encourage or facilitate money laundering. However, as evidenced by the collapse of several Ponzi fraud schemes in 2008, and several other incidents, it is clear that Jamaica is not exempt from the use by many criminals of offshore banks to

launder funds from crimes with a nexus to the United States and European countries, often with an objective of various types of tax fraud. In 2008, the former junior energy minister, and two co-defendants were indicted on money laundering, fraud and corruption charges. Also, in July 2008 four individuals were charged in connection with a large lottery scam. Due to scrutiny by banking regulators, Jamaican financial instruments are considered an unattractive mechanism for laundering money. Bulk cash smuggling of U.S. currency occurs, and funds are exchanged at a steep discount by street-side vendors. Despite efforts by the Customs Service and Tax Administration to clamp down on internal corruption, there is a significant black market for smuggled goods, which is due to tax evasion. There is a free trade zone in Montego Bay, which has a small cluster of information technology companies, and one gaming entity that focuses on international gambling. There is no indication that this free zone is being used for trade-based money laundering or terrorist financing. Domestic casino gambling, para mutual wagering and lotteries are permitted in Jamaica, and are regulated by the Betting Gaming and Lotteries Commission. In August 2008, the GOJ announced plans to license high-end casino gaming at large (1000+ room) resorts. Before these casinos open for business the GOJ must improve the regulatory capacity of its Gaming Commission to prevent criminal elements from exploiting these cash intensive businesses. Currently, casinos and other cash businesses have not been designated as subject to anti-money laundering and terrorist financing regulations. The Ministry of National Security should make this a priority.

In 2007, The GOJ passed into law the Proceeds of Crime Act (POCA), The POCA allows for both criminal and civil forfeiture and criminalizes money laundering related to narcotics offenses, fraud, firearms trafficking, human trafficking, terrorist financing and corruption, and applies to all property or assets associated with an individual convicted or suspected of involvement with a crime. This includes legitimate businesses used to launder drug money or support terrorist activity. Bank secrecy laws exist; however, there are provisions under GOJ law to enable law enforcement access to banking information. Police and Customs continue to use the Dangerous Drug Act rather than POCA to seize and forfeit (post-conviction) criminal assets. Also, there has been little, if any, use of the civil forfeiture regime enacted as part of the POCA, which is regrettable in that the law could serve as a model for forfeiture actions in other Caribbean countries. Training of investigators and prosecutors in utilizing these laws should be a priority. Jamaica initiated prosecution of its first human trafficking case in 2008.

The POCA establishes a five-year record-keeping requirement for both transactions and client identification records, and requires financial institutions to report all currency transactions over $15,000. Money transfer or remittance companies have a reporting threshold of $5,000, while for exchange bureaus the threshold is $8,000. The Customs Service has a reporting threshold of $10,000. However, data collected by Customs is not shared regularly with either the Ministry of Finance Financial Investigation Division (FID) or Tax Authorities. The POCA requires banks, credit unions, merchant banks, wire-transfer companies, exchange bureaus, mortgage companies, insurance companies, brokers and other intermediaries, securities dealers, and investment advisors to report suspicious transactions of any amount to Jamaica's financial intelligence unit (FIU), which is a unit within the Ministry of Finance's Financial Investigations Division. Based on its analysis of cash threshold reports and suspicious transaction reports (STRs), the FIU forwards cases to the Financial Crimes Unit of the FID for further investigation. There is also a Financial Crimes Division established within the Jamaica Constabulary Force, but it is unclear how its investigative responsibilities for financial crimes are shared with the Financial Crimes Unit of the FID. There is not a basis for the sharing of such information with foreign authorities, since Jamaica's FIU is not a member of the Egmont Group.

Jamaica has an ongoing education program to ensure compliance with the mandatory suspicious transaction reporting requirements. Reporting individuals are protected by law with respect to their cooperation with law enforcement entities. The FID reports that nonbank financial institutions have a

70 percent compliance rate with money laundering controls. STRs and CTRs are collected manually. There were 177 referrals to the Jamaica Constabulary Force Financial Investigative Unit. Guidelines issued by the Bank of Jamaica caution financial institutions against initiating or maintaining relationships with persons or businesses that do not meet the standards of the Financial Action Task Force (FATF).

Jamaica's central bank, the Bank of Jamaica, supervises the financial sector for compliance with anti-money laundering and counterterrorist financing provisions. In 2008 two major unregulated investment schemes, estimated to involve assets of up to $800 million, collapsed and there was an upsurge in advanced fee and lottery scams, which defrauded U.S. victims of more than $25 million. Although the POCA permits the Minister of Finance to add nonbanking institutions to the list of obligated reporting entities, the GOJ chose to wait out a lengthy court decision and did not take aggressive action to bring these nonbank institutions under its regulatory control and there are indications that these schemes were vehicles for money laundering. As a result, by the time the government moved against the institutions, the Ponzi schemes were close to collapsing. In 2008, there was an increase in the occurrence of financial crimes; however, there was not a commensurate increase in the investigation of these crimes by the FID.

Although not implicated in the theft of funds from the FID evidence vault, in early 2008, the Minister of Finance removed the FID Director and two of the FID's most experienced investigators. Since that time, the FID, which was already facing human and financial operating resource challenges, has been under reconstruction. The FID has access to data from other government sources, which include the national vehicle registry, property tax rolls, duty and transfer rolls, various tax databases, national land register, and cross border currency declarations. Direct information access to these databases is limited to a small number of people within the FID. Indirect access is available through an internal mechanism that funnels requests to authorized users. Companion legislation to the POCA, the FID Act, which would bring Jamaica's regulations fully in line with the international standards of the Egmont Group, and allow for information exchange between the FID and other FIUs remains stalled.

The POCA expands the confiscation powers of the GOJ and permits, upon conviction, the forfeiture of assets assessed to have been received by the convicted party within the six years preceding the conviction. Under the POCA, the Office of the Public Prosecutor and the FID have the authority to bring asset freezing and forfeiture orders before the court. However, both agencies are lacking in staff and resources, and few of the prosecutors have received substantive training on financial crimes. Since POCA's inception there have been four convictions for money laundering offenses and more than $1.1 million seized.

Under the POCA, forfeited assets return to the consolidated Fund. Nondrug related assets go to a consolidated or general fund, while drug related assets are placed into a forfeited asset fund, which benefits law enforcement. The Act does contemplate that forfeited assets should be distributed equally among the Ministry of National Security, the Ministry of Finance, and the Ministry of Justice. Plans to establish an Assets Recovery Agency (ARA) within the FID to manage seized and forfeited assets remain unfulfilled.

The Terrorism Prevention Act (TPA) of 2005 criminalizes the financing of terrorism, consistent with United Nations (UN) Security Council Resolution 1373. Under the Terrorism Prevention Act, the GOJ has the authority to identify, freeze, and seize terrorist finance-related assets. The FID has the responsibility for investigating terrorist financing. The FID is currently updating its FIU database and will be implementing a system to cross-reference reports from the U.S. Treasury Department's Office of Foreign Asset Control (OFAC) and the UN Sanctions Committee. Additionally, the Ministry of Foreign Affairs and Foreign Trade circulates to all relevant agencies the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee consolidated list. To date, no accounts owned by those included on the UN consolidated list have been identified in Jamaica, nor has

the GOJ encountered any misuse of charitable or nonprofit entities as conduits for the financing of terrorism. Amendments to the TPA to bring nonprofit organizations and charities within the coverage of TPA are pending, and should be passed.

The Government of Jamaica appointed an action-oriented Commissioner of Customs in 2008 who has worked to control trade based money laundering, tax evasion, and corruption.

Jamaica and the United States have a Mutual Legal Assistance Treaty (MLAT) that entered into force in 1995, as well as an agreement for the sharing of forfeited assets, which became effective in 2001. In July 2008, Norris Nembhard, a designated foreign narcotics kingpin under the Foreign Narcotics Kingpin Act was extradited to the United States and the National Commercial Bank was charged with violations of the Money Laundering Act involving $27 million of Nembhard's drug proceeds. Jamaica is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. Jamaica is a member of the Caribbean Financial Action Task Force (CFATF), a FATF-style regional body, and the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Until the FID Act is passed, the FID will not meet the membership requirements of the Egmont Group.

The Government of Jamaica should move to improve regulatory and oversight capacities before establishing an offshore financial center and licensing high-end casino gaming. The GOJ should ensure the swift passage of the FID Act to qualify the FIU to meet the international standards for membership in the Egmont group and exchange information with other FIUs. Without a strong FID, with staff vetted to international standards, the GOJ will continue to have only limited success in attacking and dismantling organized crime through the seizure and civil forfeiture of criminal assets. In addition, the GOJ must provide the FID with strong, politically independent leadership and grant its Director the adequate resources needed to enable the FID to vet, hire, and train an appropriate number of staff for the additional work it now faces with the implementation of the POCA. The GOJ should also ensure that a duality of functions does not exist in the investigative responsibilities of the Financial Crimes Unit of the FID and the Financial Crimes Division of the Jamaican Constabulary Force.

Japan

Japan is the world's second largest economy. Although the Japanese government continues to strengthen legal institutions to permit more effective enforcement of financial transaction laws, Japan still faces substantial risk of money laundering by organized crime and other domestic and international criminal elements. In general, the domestic crime rate is very low in Japan and the police are well aware of the money laundering (ML) schemes used in Japan. According to the National Police Agency (NPA), most of the narcotics consumed are smuggled in from overseas and often distributed by criminal organizations, including the Boryokudan, commonly known in the English-speaking world as "yakuza." U.S. law enforcement investigations periodically show a link between drug-related money laundering activities in the U.S. and bank accounts in Japan. In 2006, organized crime groups were involved in around 40 percent of the money laundering cases. The major sources of illicit proceeds include prostitution, illicit gambling and "loan-sharking." Recently, remittance frauds have been discovered, some of them also involve organized crime groups.

Financial fraud schemes are increasing in Japan. There are four major types of fraud: i) "Ore-ore fraud" where phone calls are made to victims by swindlers pretending to be a relative, police officer, or practicing attorney under the pretext that they immediately need money to pay for something such as an automobile accident, and convince victims to transfer the money to a certain savings account; ii) fictitious billing fraud uses postal services or the Internet to send documents or e-mails demanding money and valuables based on fictitious bills, by which the general public is sometimes persuaded to

transfer money to designated accounts; iii) loan-guarantee fraud is a method of fraud where a letter supposedly meant as a proposal is sent to the victim, persuading the victim to transfer money to designated accounts under the pretext of a guarantee deposit for loans and iv) refund fraud where swindlers pretending to be tax officers instruct people on the procedure for tax refunds and have victims use ATMs to transfer money to designated accounts.

In 2008 Japan underwent its third comprehensive FATF Mutual Evaluation of its implementation of the 40 plus 9 recommendations. Japan's FATF review concluded that Japan was fully compliant with only four recommendations, with notably deficient performances on recommendations specific to financial institutions. According the FATF mutual evaluation report, some of the deficiencies include a failure to meet international standards on customer due diligence, politically exposed persons, correspondent banking, new technologies, designated nonfinancial businesses and professions, internal controls and audits, and beneficial ownership disclosures. While noting Japan's good faith efforts, among FATF's fundamental conclusions is that "more training and investigatory resources are needed for AML/CTF law enforcement authorities."

Drug-related money laundering was first criminalized under the Anti-Drug Special Law that took effect July 1992. This law also mandates the filing of suspicious transaction reports (STRs) for suspected proceeds of drug offenses and authorizes controlled drug deliveries. The legislation also creates a system to confiscate illegal profits gained through drug crimes. The seizure provisions apply to tangible and intangible assets, direct illegal profit, substitute assets, and criminally derived property that have been commingled with legitimate assets. The narrow scope of the Anti-Drug Special Law and the burden required of law enforcement to prove a direct link between money and assets to specific drug activity limits the law's effectiveness. As a result, Japanese police and prosecutors have undertaken few investigations and prosecutions of suspected money laundering. Many Japanese officials in the law enforcement community, including Japanese customs, believe that Japan's organized crime groups have been taking advantage of these limitations and have been successfully laundering drug proceeds. The FATF review notes, "The number of prosecutions regarding money laundering cases remains low, especially in light of the problems related to drug consumption and organized crime organizations located in Japan. The low number of conviction in money laundering cases, including prosecutions of legal persons, has a negative effect on the overall effectiveness of the criminalization of money laundering."

Japan expanded its money laundering law beyond narcotics trafficking to include money laundering predicate offenses such as murder, aggravated assault, extortion, theft, fraud, and kidnapping when it passed the 1999 Anti-Organized Crime Law (AOCL), which took effect in February 2000. The law extends the confiscation laws to include additional money laundering predicate offenses and value-based forfeitures, and enhances the suspicious transaction reporting system.

The AOCL was partially revised in June of 2002 by the "Act on Punishment of Financing to Offenses of Public Intimidation," which specifically added the financing of terrorism to the list of money laundering predicates. A further amendment to the AOCL was submitted to the Diet for approval in October 2005, and would expand the predicate offenses for money laundering from approximately 200 offenses to nearly 350 offenses, with almost all offenses punishable by imprisonment.

On March 29, 2007, Japan's government enacted the "Law for Prevention of Transfer of Criminal Proceeds." The legislation, designed to bring Japan into closer compliance with the FATF 40 plus 9 recommendations, marked significant changes in Japan's anti-money laundering landscape. In addition to the financial institutions previously regulated, effective March 1, 2008, the new statute expands the types of nonfinancial businesses and professions under the law's purview to include real estate agents, private mail box agencies, dealers of precious metals and stones; and certain types of trust and company service providers. Covered entities must conduct customer due diligence, confirm client identity, retain customer verification records, and report suspicious transaction reports (STRs) to the

authorities. Legal and accounting professionals such as judicial scriveners and certified public accounts are now subject to customer due diligence and record keeping, but not STR reporting. However, the law delegates CDD rulemaking to Japan Federation Bar Association, which drafted and now enforces "Rules Regarding the Verification of Clients' Identity and Record-Keeping." In its evaluation, FATF characterized these "Rules" as allowing for exemptions from CDD obligations that were "unclear" and could be "interpreted as exempting a large number of transactions from CDD."

Japan's Financial Services Agency (FSA) supervises all financial institutions. The Securities and Exchange Surveillance Commission supervises securities transactions. The FSA classifies and analyzes information on suspicious transactions reported by financial institutions, and provides law enforcement authorities with information relevant to their investigation. Japanese banks and financial institutions are required by law to record and report the identity of customers engaged in large currency transactions. There are no secrecy laws that prevent disclosure of client and ownership information to bank supervisors and law enforcement authorities.

In a high-profile 2006 court case, the Tokyo District Court ruled to acquit a Credit Suisse banker of knowingly assisting an organized crime group to launder money, despite doubts about whether the banker performed proper customer due diligence. Japanese law does not protect bankers and other financial institution employees who cooperate with law enforcement entities.

In April 2002, the Diet enacted the Law on Customer Identification and Retention of Records on Transactions with Customers by Financial Institutions (a "know your customer" law). The law reinforced and codified the customer identification and record-keeping procedures that banks had practiced for years. The Foreign Exchange and Foreign Trade law was revised in January 2007, so that financial institutions are required to make positive customer identification for both domestic transactions and transfers abroad in amounts of more than 100,000 yen (approximately $1,120). The CDD requirements of the Prevention of the Transfer of Criminal Proceeds Act, which require financial institutions to verify customer identification data for natural and legal persons, effectively prohibit the opening of anonymous accounts or account in fictitious names. Banks and financial institutions are required to maintain customer identification records for seven years. In January 2007, an amendment to the rule on Customer Identification by Financial Institutions came into force, whereby financial institutions are now required to identify the originators of wire transfers of over 100,000 yen.

The customer due diligence framework does not fully address the issue of authorized persons, representatives and beneficiaries or of beneficial ownership. There is no requirement for financial institutions to gather information on the purpose and intended nature of the business relationship or to conduct ongoing due diligence on these relationships. And since Japan is not implementing an AML/CTF risk-based approach, there are no provisions that mandate enhanced due diligence for higher-risk customers, business relationships and transactions or authorize simplified due diligence.

To facilitate the exchange of information related to suspected money laundering activity, the FSA established the Japan Financial Intelligence Office (JAFIO) on February 1, 2000, as Japan's financial intelligence unit. Under the 2007 anti-money laundering law, on April 1, 2007, JAFIO relocated from the FSA to the National Police Agency, where it is known as the Japan Financial Intelligence Center (JAFIC). The JAFIC has 41 personnel under the supervision of the Director General of Organized Crime Department and Councilor for Prevention of Money Laundering.

JAFIC receives an increasing number of STRs (approximately 99,000 in 2005, 114,000 in 2006 and more than 158,000 in 2007). It undertakes a primary analysis that involves automatic cross-matching between the STR data and other information in its databases, and then circulates approximately 60 percent of the STRs received to law enforcement agencies, including the police, public prosecutors, customs, coast guard, and the SESC (Securities and Exchange Surveillance Commission) within the FSA. The FATF Mutual Evaluation noted that the FIU needed to improve its analytic capacity and tactical and strategic analysis of STRs, using appropriate analytic tools. Reportedly, an in-depth

analysis involving the development of a comprehensive intelligence file derived from STR and including cross-matching police, administrative and open source databases, is undertaken on an increasing number of STRs. JAFIC has good access to law enforcement and other information. JAFIC receives STRs from financial institutions and specified business operators including Shinkin banks (cooperative regional financial institutions serving small and medium enterprises and local residents), insurance companies, securities companies, trust companies, financial leasing companies, credit card companies, money and currency exchangers. Since March 2008, a new electronic reporting system has been implemented which permits STRs to be sent directly to the FIU.

The main law enforcement bodies involved are the Prefectural Police and the Public Prosecutor's Office. Both are responsible for AML/CTF investigations and, according to the FATF evaluation, have adequate powers.

The Foreign Exchange and Foreign Trade Law requires travelers entering and departing Japan to report physically transported currency and monetary instruments (including securities and gold weighing over one kilogram) exceeding one million yen (approximately $11,235) or its equivalent in foreign currency, to customs authorities. Failure to submit a report, or submitting one that is false or fraudulent, can result in a fine of up to 200,000 yen (approximately $2,250) or six months' imprisonment. The declaration requirement applies only to carriage by an individual, not to other forms of physical cross border movement of currency and bearer instruments. Moreover, few resources are devoted to enforcement of cross-border currency declaration requirements. FATF underscored this ongoing area of concern, concluding, "Customs only focuses on smuggling and trafficking control and does not have AML/CTF enforcement capabilities. As a consequence, no report on cross-border currencies movements has been made to JAFIC."

In response to the events of September 11, 2001 the FSA used the anti-money laundering framework provided in the Anti-Organized Crime Law to require financial institutions to report transactions where funds appeared either to stem from criminal proceeds or to be linked to individuals and/or entities suspected to have relations with terrorist activities. The 2002 Act on Punishment of Financing of Offenses of Public Intimidation, enacted in July 2002, criminalized terrorism and terrorist financing, added terrorist financing to the list of predicate offenses for money laundering, and provided for the freezing of terrorism-related assets. The terrorism finance offense does not cover collection of funds by nonterrorists, nor does it criminalize the indirect collection or provision of funds. The law has not yet been applied, and it is unclear whether its wording covers collecting or providing funds for any purpose other than committing terrorist acts, such as to support terrorist organizations or individual terrorists. In addition, the offense is limited to "funds" and does not cover other financial and nonfinancial assets.

Terrorist financing risks in the Non-Profit Organization (NPO) sector are relatively low in Japan. According to the FATF mutual evaluation, NPOs are subject to a high degree of transparency and public accountability for their operations and there is a generally comprehensive regime of licensing, registration or oversight. While there is a wide range of national, regional and activity-specific regulators for NPOs, coordination between regulators and investigation agencies is generally effective. However, Japan has not yet conducted any specific outreach to the NPO sector to raise awareness about risks of abuse for terrorist financing and relevant AML/CTF preventive measures.

Japan has established a comprehensive mechanism to confiscate, freeze and seize the proceeds of crime; however the regime does not appear to be fully and effectively implemented. As to the freezing of terrorist assets, a system based on a licensing system prior to carrying out certain transactions has been implemented under the Foreign Exchange Act. This system does not cover domestic funds that are not intended to leave Japan, but does cover transactions in foreign currency, or with a nonresident in Japan, as well as overseas transactions. It does not allow for freezing without delay in the absence of an attempted transaction, so that financial institutions are not required to screen their customer

database and freeze designated funds or assets. For transactions in domestic currency within Japan that do not involve a nonresident, Japan can freeze terrorist funds under the Act on the Punishment of Financing of Offences of Public Intimidation and the Act on the Punishment of Organized Crime. However, this mechanism also reaches only funds, not other kinds of assets, and does not allow Japan to freeze terrorist assets without delay.

After September 11, 2001, Japan has regularly designated for asset freezing all the suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list, and have also designated a number of entities and persons of other countries listed under UNSCR 1373. However, the FATF determined that the limitations of Japan's asset freezing system, described above, result in "gaps in the implementation of the UNSCRs 1267, 1373 and successor resolutions." Japan is a party to the UN Convention for the Suppression of the Financing of Terrorism.

Underground banking systems operate widely in Japan, especially in immigrant communities. Such systems violate the Banking Law. There have been a large number of investigations into underground banking networks. Reportedly, substantial illicit proceeds have been transferred abroad, particularly to China, North and South Korea, and Peru. In November 2004, the Diet approved legislation banning the sale of bank accounts, in a bid to prevent the use of purchased accounts for fraud or money laundering.

In 2002, Japan's FSA and the U.S. Securities and Exchange Commission and Commodity Futures Trading Commission signed a nonbinding Statement of Intent (SOI) concerning cooperation and the exchange of information related to securities law violations. In January 2006 the FSA and the U.S. SEC and CFTC signed an amendment to their SOI to include financial derivatives.

Japan has not enacted laws that allow for sharing of seized narcotics assets with other countries. However, the Japanese government fully cooperates with efforts by the United States and other countries to trace and seize assets, and makes use of tips on the flow of drug-derived assets from foreign law enforcement efforts to trace funds and seize bank accounts.

Japan is a party to the 1988 UN Drug Convention but is not a party to the UN Convention against Corruption or to the UN Convention against Transnational Organized Crime. Ratification of the latter convention would require amendments to Japan's criminal code to permit charges of conspiracy, which is not currently an offense. Minority political parties and Japan's law society have blocked this amendment on at least three occasions. Japan is a member of the Financial Action Task Force and the Asia/Pacific Group against Money Laundering. The JAFIC is a member of the Egmont Group.

The Government of Japan has many legal tools and programs in place to successfully detect, investigate, and combat money laundering and terror finance. However, the number of investigations, prosecutions, and convictions for money laundering remain low in relation to the amount of illicit drugs consumed and other predicate offenses. To strengthen its AML/CTF regime, Japan should make serious efforts to follow the comprehensive recommendations in the 2008 FATF mutual evaluation. Increased emphasis should be given to combating underground financial networks that are not subject to financial transparency safeguards. Since Japan is a major trading power and the misuse of trade is often the facilitator in alternative remittance systems, underground finance, and value transfer schemes, Japan should take steps to identify and combat trade-based money laundering. Japan should also become a party to the UN Transnational Organized Crime Convention and the UN Convention against Corruption.

Jersey

The Bailiwick of Jersey (BOJ), one of the Channel Islands, is an international financial center offering a sophisticated array of offshore services. A Crown Dependency of the United Kingdom (UK), it relies on the UK for its defense and international relations. Due to Jersey's investment services, most of the

illicit money in Jersey is derived from foreign criminal activity. Political corruption and suspicious activity related to financial re-structuring of infrastructure industries such as oil, gas and transportation are emerging trends. Money laundering mostly occurs within Jersey's banking system, investment companies, and local trust companies.

The financial services industry is a key sector and provides 60 percent of Jersey's gross domestic product. It consists of 51 banks; 1,452 funds; trust companies; money services businesses (MSBs); and insurance companies, which are largely captive insurance companies. The menu of services includes investment advice, dealing management companies, and mutual fund companies. In addition to financial services, companies offer corporate services, such as special purpose vehicles for debt restructuring and employee share ownership schemes. For high net worth individuals, there are wealth management services. All regulated entities can sell their services to both residents and nonresidents. All financial businesses must have a presence in Jersey, and management must also be in Jersey. However, although Jersey does not provide offshore licenses, it administers a number of companies registered in other jurisdictions. These companies, known as "exempt companies," do not pay Jersey income tax and their services are only available to nonresidents. Alternate remittance systems do not appear to be prevalent in Jersey.

In October 2008, the International Monetary Fund (IMF) assessed Jersey's anti-money laundering /counterterrorist financing (AML/CTF) regime as well as the banking, insurance and securities sectors; the results are expected to be published in 2009. In anticipation of the assessment, Jersey took numerous steps to enhance its AML/CTF regime to bring it into greater compliance with the Financial Action Task Force (FATF) standards through issuance of consultation and position papers; enactment of new primary and secondary legislation, key amendments, orders, and regulations; and outreach to regulated entities.

The AML/CTF Strategy Group was established in Jersey in 2007 to provide a forum for the Jersey agencies represented on the group to liaise, discuss and develop coordinated strategies and policies to enhance Jersey's capability to prevent and detect financial crime and terrorist financing. The Strategy Group is chaired by the Chief Executive of the States, and the financial Services Commission (FSC) provides the secretariat for the group. The group comprises officers from the following government departments and agencies: the Chief Minister's Department, the Economic Development Department, the Law Officers' Department, the Joint Financial Crimes Unit, the Police Force, the Customs and Immigration Service, the FSC, and the Shadow Gambling Commission.

Jersey's main anti-money laundering (AML) laws are the Drug Trafficking Offenses (Jersey) Law 1988, which criminalizes money laundering related to narcotics trafficking; and the Proceeds of Crime (Jersey) Law 1999 (POCL), which extends the predicate offenses for money laundering to all offenses punishable by at least one year in prison. Both laws were amended in 2008 to enhance various provisions, including those regarding the failure to report knowledge or suspicion of money laundering and the enforcement of external confiscation orders. Also, the Money Laundering (Jersey) Order 2008, issued pursuant to the POCL, contains detailed provisions addressing several preventive measures, including customer due diligence measures and recordkeeping and reporting requirements. Additionally, in September 2008, the Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008 came into force and provides for one or more supervisory bodies to be tasked with monitoring, and ensuring AML/CTF compliance by lawyers, accountants, estate agents and high-value goods dealers who take cash payments of more than 15,000 euros (approximately $20,250) per transaction or linked transactions, or their sterling equivalent.

The Corruption (Jersey) Law 2005 came into force in February 2007. Certain definitions contained in Articles 2, 3, and 4 of this law were amended in November 2007.

On July 1, 2005, the European Union Savings Tax Directive (ESD) came into force. The ESD is an agreement between the Member States of the European Union (EU) to automatically exchange

information with other Member States about EU tax resident individuals who earn income in one EU Member State but reside in another. Although not part of the EU, the three UK Crown Dependencies (Jersey, Guernsey and Isle of Man) have voluntarily agreed to apply the same measures as those in the ESD and have elected to implement the withholding tax option (also known as the "retention tax option") within the Crown Dependencies.

The Jersey Economic Development Department is the government body responsible for administering the law, and regulating, supervising, promoting, and developing Jersey's finance industry. The FSC is the financial services regulator. The FSC formed a dedicated AML Unit to lead Jersey's operational AML/CTF strategy. The AML Unit is responsible for monitoring compliance with legislation and Codes of Practice by MSBs such as bureaux de change, check cashers, and money transmitters; lawyers; accountants; estate agents; high-value goods dealers; and nonprofit organizations. The AML Unit also supports the FSC's Supervision Divisions, which are responsible for oversight of businesses supervised by the FSC with the exception of MSBs. Jersey's law enforcement and regulatory agencies have extensive powers to cooperate with one another, and regularly do so. The FSC cooperates with regulatory authorities, for example, to ensure that financial institutions meet AML obligations.

Approximately 33,000 Jersey companies have registered with the Registrar of Companies, the Director General of the FSC. In addition to public filing requirements relating to shareholders, the FSC requires each company to provide the FSC with details of the ultimate individual beneficial owner of each Jersey-registered company. The Registrar keeps the information in confidence.

Following extensive consultation with the Funds Sector, and approval by the State of Jersey in November 2007, the FSC published Codes of Practice for Fund Services Business. The Code consists of seven high level principles for the conduct of fund services business, together with more detailed requirements in relation to each principle.

Financial institutions must report suspicious transactions under the narcotics trafficking, terrorism, and AML laws. There is no threshold for filing a suspicious activity report (SAR), and the reporting individual is protected from criminal and civil charges by safe harbor provisions in the law. Banks and other financial service companies must maintain financial records of their customers for a minimum of ten years after completion of business.

The Joint Financial Crimes Unit (JFCU), Jersey's financial intelligence unit (FIU), includes Jersey Police and Customs officers. The FIU is responsible for receiving, investigating, and disseminating SARs. In 2007, the JFCU received 1,517 SARs, the majority of which were received from banks, although a growing number are submitted by fund managers. Approximately 25 percent of the SARs filed result in further police investigations. Reports filed in the first six months of 2007 indicate a 32 percent increase in the number of SARs submitted to the JFCU by financial institutions compared to the three-year average for this same period. In the first six months of 2007, Jersey held more than 2.5 million pounds (approximately $4,900,000) in bank or trust company accounts pending police investigation of suspicious activity. The FIU also responds to requests for financial information from other FIUs. In 2007, the JFCU received 687 requests for assistance from counterparts in other jurisdictions.

The JFCU, in conjunction with the Attorney Generals Office, traces, seizes and freezes assets. A confiscation order can be obtained if the link to a crime is proven. If the criminal has benefited from a crime, legitimate assets can be forfeited to meet a confiscation order. Assets may be frozen for an indefinite period. Frozen assets are confiscated by the Attorney General's Office on application to the Court. Proceeds from asset seizures and forfeitures are placed in two funds. Drug-trafficking proceeds go to one fund, and the proceeds of other crimes go to the second fund. The drug-trafficking funds are used to support harm reduction programs and education initiatives, and to assist law enforcement in the fight against drug-trafficking. Only limited civil forfeiture is allowed in relation to cash proceeds of drug-trafficking located at the ports.

Jersey criminalizes money laundering related to terrorist activity through the Prevention of Terrorism (Jersey) Law 1996. The Terrorism (Jersey) Law 2002, which entered into force in January 2003, and was amended in 2008, enhances the powers of the authorities to investigate terrorist offenses, to cooperate with law enforcement agencies in other jurisdictions, and to seize assets. Jersey does not circulate the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list, nor any other government's lists, although the FSC website has links to various websites that contain such. In addition, the Chief Minister's Department website includes a page for international sanctions that includes links to the UN and U.K. consolidated lists, the latter of which includes all of the persons listed in the UN consolidated list, as well as EU and UK designations. Jersey expects its institutions to gather information on designated entities from these or other Internet websites, and other public sources. Jersey authorities have instituted sanction orders freezing accounts of individuals connected with terrorist activity.

In August 2008, the Non-Profit Organizations (Jersey) Law of 2008 came into force. The law provides for the registration and monitoring of nonprofit organizations by the FSC and is specifically designed to prevent and combat the misuse of nonprofit organizations by terrorists. The FSC plans to do further work with the sector to include issuing publications, conducting training, and coordinating with relevant organizations such as the Association of Jersey Charities.

Jersey signed the Tax Information Exchange Agreement (TIEA) with the United States in 2002, and plans to sign the same agreements with other countries, thus meeting international obligations to cooperate in financial investigations. The FSC has reached agreements on information exchange with securities regulators in Germany, France, and the United States; and has a memorandum of understanding for information exchange with Belgium. Registrar information is available, under appropriate circumstances and in accordance with the law, to U.S. and other investigators. In 2007, the FSC signed a memorandum of understanding with the British Virgin Islands Financial Services Commission that will further cooperation between the two regulatory bodies.

Application of the 1988 UN Drug Convention was extended to Jersey on July 7, 1997. Jersey is a member of the Offshore Group of Insurance Supervisors (OGIS) and the Offshore Group of Banking Supervisors (OGBS). It works with the Basel Committee on Banking Supervision and the Financial Action Task Force. The JFCU is a member of the Egmont Group.

The Bailiwick of Jersey should continue to enhance compliance with international standards. The FSC should ensure the AML Unit has enough resources to function effectively, and to provide outreach and guidance to the sectors it regulates, especially the newest entities required to file reports. The FSC should distribute the UN lists of designated terrorists and terrorist organizations to the obliged entities and not expect the entities to stay current through their own Internet research.

Jordan

Jordan is not a regional or offshore financial center and is not considered a major venue for international criminal activity. Jordan does have a well developed financial sector with significant banking relationships in the Middle-East. Jordan's long and remote desert borders and nexus to Iraq, Syria, and the West Bank make it susceptible to the smuggling of bulk cash, fuel, narcotics, cigarettes, and counterfeit goods and contraband, although there is insufficient information available from the Government of Jordan (GOJ) to quantify these crimes.

Jordan boasts a thriving "import-export" community of brokers, traders, and entrepreneurs that regionally are involved with value transfer via trade and customs fraud. Illicit narcotics, psychotropic substances, and chemical precursors are not known to be major components of criminality in Jordan. There are some indications of use of Jordan for money laundering of illicit funds derived from narcotics activity in the U.S. and possibly Europe via bulk cash smuggling for criminal elements

involving Jordanians in those areas. However, it is thought that the major sources of illicit funds in Jordan are most likely to be related to customs fraud, tax fraud and intellectual property rights (IPR) violations due to Jordan's dependence on imports and its limited natural resources and manufacturing base. A wide array of pirated or counterfeit goods is for sale on the streets of Jordan. One phenomenon that surfaced during 2008 was the use of gold in lieu of cash for movement of liquid assets. The scheme involves persons crossing into Jordan at land and seaports, making an admission of trying to enter multi-kilo quantities of gold to inspecting customs authorities, paying a fine and then re-exporting the gold at the entry point thus creating a declaration document to lend legitimacy to the movement of the high-value precious metal.

Inquiries and assessments conducted during 2008 reveal that Jordan is vulnerable to trade-based money laundering, bulk cash smuggling, and alternate remittance systems. Data on the prevalence of these activities was not available for two reasons: recognition of these methodologies in Jordan is relatively new; and it is a common practice in Jordan for individuals and businesses of all types to first contact the General Intelligence Directorate if suspicions of certain crimes surface. Offenses that the populace perceives as crimes relating to national security fall into that category. Money laundering and terrorist financing are categorized in this way. Details of these cases are rarely published or revealed. In 2008, there was an increase in securities-related financial crimes due to the discovery of a number of major Ponzi schemes in which thousands of investors lost investments. By year's end there were over 50,000 complaints filed relating to these schemes. Although the GOJ has revealed no indicators of the use of hawala or other alternative remittance systems, Jordan's sizeable foreign worker population and Jordanian enclaves in the U.S., Europe, and Arabian Gulf countries, and are thought to use this form of cash transfer methodology to move legal and illicit funds both out of and into Jordan.

In August 2001, the Central Bank of Jordan (CBJ), which regulates Jordan's 27 banks as well as its financial institutions, including money services businesses, issued anti-money laundering regulations designed to meet some of the FATF 40 Recommendations on Money Laundering. Subsequently, money laundering has been considered an "unlawful activity" subject to criminal prosecution. Jordan's banking laws prohibit registration of offshore banks or shell companies. In 2002, money laundering was criminalized related to insurance operations.

On July 17, 2007, Jordan enacted Law No. 46 for the Year 2007—the Anti Money Laundering Law (AML) that criminalizes money laundering. The AML Law does not cover financing of terrorism, but it criminalizes money laundering and stipulates as predicate offenses to that crime all felony crimes or any crime stated in international agreements to which Jordan is a party whether such crimes are committed inside or outside the Kingdom, provided that the act committed is subject to criminal penalty in the country in which it occurs. Felony crimes are those for which a penalty of three years or more of incarceration is attached. With this approach, several of the 20 crimes recommended by the FATF for inclusion in AML legislation do not meet the penalty level for major crimes and therefore are excluded as predicate offenses for money laundering under Jordan's current AML Law. The most noteworthy of these are: financing of terrorism, smuggling, extortion, intellectual property rights violations, sexual exploitation of children, trafficking in persons, trafficking in stolen property, and environmental crimes. The Banking Law of 2000 (as amended in 2003) allows judges to waive bank secrecy provisions in any number of criminal cases, including suspected money laundering and terrorist financing. The AML Law provides immunity against confidentiality sanctions for obligated entities that report suspicious transactions based on the AML Law. The effectiveness of the AML Law remains untested as there have been no prosecutions for money laundering based on either the CBJ regulations or the AML Law.

The AML law created the National Committee on Anti-Money Laundering (NCAML) as well as the Anti-Money Laundering Unit (AMLU) as Jordan's financial intelligence unit. The NCAML is chaired by the Governor of the Central Bank of Jordan and has as members: a Deputy Governor of the Central Bank named by the CBJ Governor to serve as deputy chairman of the committee, the Secretary

General of the Ministry of Justice, the Secretary General of the Ministry of the Interior, the Secretary General of the Ministry of Finance, the Secretary General of the Ministry of Social Development (which overseas charitable organizations), the Director of the Insurance Commission, the Controller General of Companies, a Commissioner of the Securities Commission, and the head of the Anti-Money Laundering Unit. The NCAML is responsible for: formulating general AML policy, supervising the implementation of tasks of the AMLU, facilitating and coordinating exchange of information related to money laundering, participating in international fora, proposing necessary regulations for implementation of the AML Law, coordinating and assigning competent parties to generate statistical reports related to the AML program of the GOJ, and approving and adopting a budget for the AMLU.

The Ministries of Justice, Interior, Finance, and Social Development, as well as the Insurance Commission, Controller General of Companies, and Jordan Securities Commission all have a part in regulating various other nonfinancial institutions through issued regulations and instructions. The AMLU is obligated to work with these entities to ensure that comprehensive anti-money laundering/countering the financing of terrorism (AML/CTF) approach is undertaken in keeping with international standards and best practices. Of the regulatory entities of the GOJ, the Central Bank of Jordan, the Jordan Securities Commission, and the Insurance Commission of Jordan are best staffed and trained to conduct compliance investigations. These entities have issued implementing instructions to the regulated entities under their purview concerning AML/CTF requirements, which have the force of law. The extent of the use of the formal financial system for money laundering or terrorist financing is difficult to measure due to the lack of reporting data available that clearly identifies these offenses. Since the AML Law is still relatively new, some agencies of these cabinet level entities lack coordination in the overall AML/CTF effort in Jordan.

The CBJ has a well developed bank supervision department whose procedures, until the recent past, focused almost exclusively on safety and soundness. However, the CBJ did instruct financial institutions to be particularly careful when handling foreign currency transactions, especially if the amounts involved are large or if the source of funds is in question. The AML Law requires obligated entities to: undertake due diligence in identifying customers; refrain from dealing with anonymous persons or shell banks; report any suspicious transaction to the AMLU; and comply with instructions issued by competent regulatory parties to implement provisions of the law. The CBJ drafted an AML/CTF dedicated bank examination manual in 2008, but had not officially adopted it by the end of the year.

Financial institutions are required under the AML Law to report all suspicious transactions whether the transaction was completed or not via suspicious transaction reports (STRs) sent to the AMLU. Entities required to report suspicious transactions include: banks, foreign exchange companies, money transfer companies, stock brokerages, insurance companies, credit companies, and any company whose articles of association state that its activities include debt collection and payment services, leasing services, investment and financial asset management companies, real estate trading and development entities, and companies trading in precious metals and stones. Lawyers and accountants are not considered to be obligated entities under the law.

All obligated entities are required to conduct due diligence to identify customers; their activities, legal status, and beneficiaries; and follow-up on transactions that are conducted through an ongoing relationship. Business dealings with anonymous persons, persons using fictitious names or shell banks are prohibited. Obligated entities are required to comply with instructions issued by competent regulatory authorities as listed in the law. Disclosure to the customer or the customer's beneficiary of STRs and/or verifications or investigations by competent authorities is prohibited. They are also required to respond to any inquiry from the AMLU regarding STRs or requests for assistance from other competent judicial, regulatory, administrative, or security authorities needing information to perform their responsibilities.

GOJ officials report that financial institutions have been filing suspicious transaction reports and cooperate with prosecutors' requests for information related to narcotics trafficking and terrorism cases. Most reporting is done by banking institutions which have well-developed AML compliance programs. During 2008, only a few STRs came from all the other types of obligated entities. There were no arrests or convictions for money laundering or terrorist financing in Jordan in 2008. The standard for forwarding STRs is a potential problem in the existing law and will require significant outreach resources to educate obligated entities. The banking, securities, and insurance sectors are the best regulated obligated entities and those that have been best educated regarding recognizing indicators of money laundering and terrorist financing, but there is still much to be done with the other obligated sectors. The money services business (MSB) sector is the riskiest obligated sector and lacks sufficient regulatory oversight and verification of compliance with reporting suspicious transactions of the AML Law. Real estate businesses and precious metals and stones dealers are also under-regulated and are generally unknowledgeable of their responsibilities to report suspicious transactions. Charitable associations, although not specified as obligated entities, occupy another troublesome sector, which requires better regulatory supervision and oversight. There are over 1,000 nonprofit organizations registered in Jordan, the majority of which are charitable organizations. Oversight responsibility for these rests with the Ministry of Social Development, which is understaffed and incapable of verifying the financial activities of all of the organizations. A new Associations Law is currently in the legislative process; however, its provisions to safeguard against abuse for money laundering and terrorist financing may be insufficient.

The AMLU was formed immediately upon passage and enactment of the AML Law. The financial intelligence unit is designated by law as an independent entity within the organizational structure of the Central Bank of Jordan. It is also physically located in and operationally funded for 2009 by the CBJ. The AMLU also uses the CBJ server and database for all information technology needs. The AMLU was staffed with the same personnel that made up the CBJ's Suspicious Transaction Follow-Up Unit, in existence for several years, and is composed of a director, an outreach officer, one attorney, and one analyst. Since the enactment of the AML Law, there has been no increase in staffing of the AMLU. A comprehensive FIU development plan was informally adopted for the AMLU prior to the implementation of the AML Law. However, follow-through on this plan has been stymied due to administrative hurdles. In order for the AMLU to be fully staffed, funded, and functional, by-laws governing its administration must be approved by the NCAML, submitted to the GOJ Cabinet, and published in Jordan's Official Gazette. The NCAML did not approve the by-laws until September 2008 at which time they were forwarded to the GOJ Cabinet for ratification and implementing procedures. By the end of 2008, the AMLU by-laws had not been ratified by the Cabinet. Until the AMLU by-laws are published in the Official Gazette, the personnel assigned to the AMLU remain employees of the CBJ seconded to the AMLU and no additional personnel may be hired. Plans to second additional analysts to the AMLU from other GOJ agencies have not materialized. Due to the absence of legally established administrative by-laws, the AMLU director seeks the approval of the Governor or Vice-Governor of the CBJ for administrative decisions. These conditions have raised questions concerning AMLU independence and freedom from political influence as an FIU. Although the AMLU has made overtures to sponsoring countries stating its desire to become a member of the Egmont Group of Financial Intelligence Units, it is unlikely that it can gain membership until 2011 at the earliest.

The AMLU is organized on a general administrative FIU model and is responsible for receiving STRs from the obligated entities designated in the AML Law, analyzing them, requesting additional information related to the reported activity and forwarding the information to the prosecutor general for further action if there is sufficient cause to believe the transaction is related to money laundering or other financial crime activity. The AMLU does not have criminal investigative and/or direct regulatory responsibility, but it is authorized to require any information needed from obligated entities stipulated in the AML Law considered necessary for the performance of its duties if the needed information is

related to information already received by the AMLU. Involvement of the AMLU in assisting criminal investigations is dependent on the will of public prosecutors to use it. It is authorized to request and coordinate with judicial parties, regulatory and supervisory authorities, and security (law enforcement) authorities. Suspicious transactions identified as potentially related to terrorist financing are outside of the AMLU's purview.

At the end of 2008, the AMLU continued to work toward establishment of formal ties through memoranda of understanding with competent GOJ authorities possessing the necessary databases and records pertinent to pursuing financial intelligence analysis and money laundering investigations. The AMLU received approximately 160 STRs in 2008 of which five were forwarded to prosecutors for further action. Only two of those indicated the possibility of money laundering. No prosecutions for money laundering have occurred in Jordan since the enactment of the 2007 AML law. Due to lack of knowledge of the AML law, uncertainty about the role of the AMLU with its limited personnel and functional capability, few prosecutors have considered using the AMLU to assist in criminal prosecutions or to charge financial crime violators with money laundering.

One significant challenge facing the GOJ is determining how law enforcement entities are tasked to conduct financial investigations relating to money laundering and terrorist financing. Since the AML law was only implemented in July 2007, law enforcement agencies and public prosecutors are still deliberating the issue. There is no specific GOJ agency designated as the lead entity for investigating financial crimes. Although the AMLU is required by law to forward findings developed from STRs to the public prosecutors of the Ministry of Justice, prosecutors of the State Security court also investigate and prosecute financial crimes, particularly those that deal with national security. In Jordan, a civil law country, prosecutors lead all criminal investigations. Investigative field work needed by prosecutors for criminal investigations is shared between several GOJ law enforcement agencies dependent on the predicate offense generating money laundering activity: the Public Security Department (PSD—national police service), the General Intelligence Directorate (GID—both a criminal investigative agency and intelligence service; investigation of all terrorist activity falls to the GID), and the Directorate of Military Security (DMS) of the Jordan Armed Forces. Jordan Customs also conducts criminal investigations and has its own prosecutors, but penalties for customs violations fall below the level of a major crime (penalty in excess of three years). Nearly all customs violations including commercial fraud are decided as administrative cases and seldom accrue criminal penalties including incarceration. The concept of forwarding large monetary value customs fraud cases to public prosecutors for criminal investigation and prosecution has not taken root in Jordan's legal system. This anomaly leaves the possibility of forfeiture of proceeds of customs related criminal activity to the Kingdom totally unexploited.

Notwithstanding the lack of emphasis on pursuing money laundering or terrorist financing investigations, the GOJ has welcomed training to learn how to do so. During 2008, approximately 250 criminal investigators, prosecutors, financial sector regulators and customs officials were trained in recognizing money laundering and terrorist financing typologies. Of those 250, approximately 154 criminal investigators, prosecutors, judges, and customs officers were trained in using financial investigative techniques in investigations. In each training event, AMLU personnel assisted in training participants on the function of the AMLU and FIUs in general.

There are six public free trade zones in Jordan: the Zarqa Free Zone, the Sahab Free Zone, the Queen Alia International Airport Free Zone, the Al-Karak Free Zone, the Al-Karama Free Zone, and the Aqaba Special Economic Zone (ASEZ). All six list their investment activities as "industrial, commercial, service, and tourist." There are 32 private free trade zones, a number of which are related to the aviation industry. Other free trade zones list their activities as industrial, agricultural, pharmaceutical, training of human capital, and multi-purpose. With the exception of ASEZ, all free trade zones are regulated by the Jordan Free Zones Corporation in the Ministry of Finance and are guided by the Law of Free Zones Corporation No. 32 for 1984 (and amendments). Regulations state

that companies and individuals using the zones must be identified and registered with the Corporation. The Aqaba Special Economic Zone is controlled by a ministerial level authority. The Aqaba Special Economic Zone Authority (ASEZA) encompasses all of the port city of Aqaba and is bounded by Saudi Arabia on the south, Israel on the west and is a short ferry ride across the Gulf of Aqaba (Red Sea) to Egypt. ASEZA has its own customs authority, which operates separately from Jordan Customs and processes all merchandise and commodities destined for businesses in the zone. It also processes all passengers entering the zone. Jordan Customs processes all shipments of goods in transit to areas outside the zone. Awareness of the methodologies and threat of trade-based money laundering and bulk cash smuggling is lacking on the part of both ASEZA Customs and Jordan Customs. However, both entities have taken steps to improve inspection and control procedures to detect these crimes. Thus far there have been no criminal cases involving the free trade zones of Jordan that indicate they were used for trade-based money laundering or bulk cash smuggling.

The 2007 AML law requires reporting of inbound cross-border movement of money if the value exceeds a threshold amount set by the NCAML. The threshold amount was set by the NCAML at 10,000 Jordanian Dinars (approximately $14,200). However, the threshold amount has not been officially established or transmitted to border control authorities for enforcement. The law also provides for the creation of cross-border currency and monetary instruments declaration forms, and although a multi-agency committee has worked on the creation of the form since the passage of the AML Law, it was not in publication by the end of 2008. The declaration requirement applies only to the entry of money into the Kingdom and not exiting. Jordan Customs is responsible for archiving the declaration forms once implemented. By the end of 2008, no mechanism had been set up to either enforce the cross border declaration requirements of the AML Law. In December 2004, the United States and Jordan signed an Agreement regarding Mutual Assistance between their Customs Administrations that provides for mutual assistance with respect to customs offenses and the sharing and disposition of forfeited assets. Collaboration on mutual money laundering related customs cases has been sparse and has been limited mostly to minimal intelligence sharing. The AML Law authorizes Customs "to seize or restrain" undeclared money crossing the border and report it to the AMLU which will decide whether the money should be returned or the case referred to the judiciary. In all known cases of detention of undeclared funds discovered during customs processing, the money has been returned to the importer.

Seizure and forfeiture of assets related to criminal activity including money laundering and terrorist financing are authorized under a combination of statutes principal of which are: the Penal Code, the Economic Crimes Law, the Anti Money Laundering Law, the Narcotics and Psychotropic Substances Law and the Prevention of Terrorism Act of 2006. Jordan's Anti-drugs Law allows the courts to seize proceeds and instrumentalities of crime derived from acts proscribed by the law. The Economic Crimes Law gives both prosecutors and the courts the authority to seize from any person proceeds generated by criminal activity under that law for a period of three months while an investigation is underway. Jordan's penal code further provides prosecutors the authority to confiscate "all things" derived from a felony or intended misdemeanor. GOJ officials claim that Jordan's cornucopia of seizure laws is sufficient to accomplish the purposes of FATF Recommendation 3 regarding authority to "confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value . . ." These statutes concentrate primarily on the proceeds of crime and not the means or instrumentalities used to commit a predicate offense to money laundering or the financing of terrorism. The multi-statute approach to freezing, confiscating or seizing of assets makes it unclear as to whether investigators may specifically trace and seize assets related to criminal activity. The GOJ has been advised by both Council of Europe and U.S. Government advisors that since this position is untested, it would be better to amend current or draft new legislation which clearly complies with FATF Recommendation 3. The GOJ publishes no statistics related to freezing, seizing, forfeiting, or confiscating the proceeds or instrumentalities of crime, and it is believed that there is no tracking

mechanism for such since there is not a statutory provision for an asset forfeiture fund or civil forfeiture in Jordan.

An October 8, 2001 revision to the Penal Code criminalized terrorist activities and the financing of terrorist acts. The Prevention of Terrorism Act of 2006 also prohibits the financing of terrorist acts. However, Jordan has no legislation that prohibits financing of terrorist organizations or groups. Guidelines issued by the CBJ state that banks should research all sanctions lists relating to terrorist financing including those issued by individual countries and other relevant authorities. The Central Bank may not circulate names on sanctions lists to banks unless the names are included on the UNSCR 1267 Sanctions Committee's consolidated list. No such assets have been identified to date. Banks and other financial institutions are required to maintain records for a period of five years in order to facilitate investigations.

Jordan is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. Jordan has signed but has yet to ratify the UN Convention against Transnational Organized Crime. Jordan is a charter member of the Middle East and North Africa Financial Action Task Force (MENAFATF) and in 2007 Jordan held the presidency of MENAFATF. The GOJ received a MENAFATF Mutual Evaluation in July 2008. The report of that evaluation will not become public until the MENAFATF plenary session in spring 2009, but it is anticipated that a multitude of deficiencies will be detailed.

The new AML Law provides judicial authorities the legal basis to cooperate with foreign judicial authorities in providing assistance in foreign investigations, extradition, and freezing and seizing of funds related to money laundering in accordance with current legislation and bilateral or multilateral agreements to which Jordan is a part based on reciprocity. Judicial authorities may order implementation of requests by foreign judicial authorities to confiscate proceeds of crime relating to money laundering and to distribute such proceeds in accordance with bilateral or multilateral agreements. There was no indication in 2008 that these provisions of the AML Law have been used by the GOJ.

In light of identified statutory and procedural deficiencies, the Government of Jordan's NCAML and the AMLU should conduct a comprehensive evaluation of Jordan's capabilities in preventing money laundering and enforcing its new law in accordance with international standards and best practices. Sufficient time has passed since the implementation of the AML Law for the GOJ to have accomplished numerous steps in its FIU implementation plan, but there has been little advancement in the AML/CTF regime. Many of the steps in the FIU implementation plan require action or approval of the NCAML which has not steadily moved forward in addressing the necessary requirements needed for compliance with the FATF 40+9 recommendations. In spite of numerous criminal cases involving large financial value, no prosecutions of money laundering have occurred since the passage of the AML Law. GOJ prosecutorial, law enforcement and customs entities should examine forms of bulk cash smuggling relating to terrorist financing and trade-based money laundering and incorporate prevention and investigative strategies that meet the requirements of complex financial investigations. These entities should also request the NCAML and the GOJ Cabinet to move ahead aggressively in approving the AMLU by-laws so that this unit can assume its vital role in assisting criminal investigations. Jordan should also establish and implement a viable asset forfeiture regime, Charitable and nonprofit organizations should have better supervision and oversight. Per FATF Special Recommendation IX, Jordan's cross-border currency reporting should include outbound declarations. Jordan should become a party to the UN Convention against Transnational Organized Crime and should draft, pass and implement legislation which meets international standards concerning the financing of terrorism as it is committed to do by virtue of its membership in the United Nations and in MENAFATF. The AML Law should be amended to include as predicate offenses to money laundering all crimes indicated by the FATF Forty Recommendations as well as any offense or act that causes a loss of revenue to the Kingdom in excess of 10,000 Jordanian Dinars (approximately

$14,200). Many offenses that generate large illicit sums that are currently outside of the reach of the AML Law's definition of money laundering could be targeted. This would improve the financial sector in Jordan thus helping the Kingdom to comport with international standards.

Kenya

Kenya is developing into a major money laundering country with an undetermined amount of narcotics proceeds laundered—the effect of increasing drug abuse especially in Coast Province and Nairobi. Kenya's use as a transit point for international drug traffickers is increasing. Kenya serves as the major transit country for Uganda, Tanzania, Rwanda, Burundi, northern Democratic Republic of Congo (DRC), and Southern Sudan. Goods marked for transit to these northern corridor countries avoid Kenyan customs duties, but authorities acknowledge that they are sold in Kenya. There is a black market for smuggled goods in Kenya. Many entities in Kenya are involved in exporting and importing goods, including nonprofit entities. Kenya has no offshore banking or Free Trade Zones.

As a regional financial and trade center for Eastern, Central, and Southern Africa, Kenya's economy has large formal and informal sectors. Annual remittances from expatriate Kenyans are estimated at $570 million to $1 billion. Residents of Kenya, including foreigners, also transfer money into and out of Kenya. Nairobi's Eastleigh Estate has become an informal remittance hub for the Somali diaspora, transmitting millions of dollars every day from Europe, Canada and the U.S. to points throughout Somalia. Although banks, wire services and other formal channels execute funds transfers, there are also thriving, informal networks of hawala and other alternative remittance systems using cash-based, unreported transfers that the Government of Kenya (GOK) cannot track. Expatriates, in particular the large Somali refugee population, primarily use hawala to send and receive remittances internationally.

The GOK has not passed a law that explicitly outlaws money laundering and creates a financial intelligence unit (FIU). The most recent legislation regarding drugs is the Criminal Procedure Code (Amendment) Bill passed in Parliament on December 16, 2008 which seeks to strengthen the definition of "drug-related offense" However, this bill does not address the criminalization of proceeds from the sale of illegal drugs and by the end of 2008, had not yet been signed into law by the President.

Section 49 of the Narcotic Drugs and Psychotropic Substance Control Act of 1994 criminalizes money laundering related to narcotics trafficking. The offense is punishable by a maximum prison sentence of 14 years. However, Kenya has never had a conviction for the laundering of proceeds from narcotics trafficking. The GOK has cobbled together a series of laws and guidance, including the 1994 Act, Legal Notice No. 4 of 2001, the Central Bank of Kenya (CBK) Guidelines on Prevention of Money Laundering, and enabling provisions of other laws that it uses to fight money laundering. However, Kenya has not developed an effective anti-money laundering (AML) regime.

In November 2006, the GOK published a proposed Proceeds of Crime and Anti-Money Laundering Bill, a revised version of a 2004 law. The proposed law declares itself to be "An act of Parliament to provide for the offence of money laundering and to introduce measures for combating the offence, to provide for the identification, tracing, freezing, seizure and confiscation of the proceeds of crime." It defines "proceeds of crime" as any property or economic advantage derived or realized, directly or indirectly, as a result of or in connection with an offence. The draft legislation provides for criminal and civil restraint, seizure and forfeiture. In addition, the proposed bill authorizes the establishment of an FIU and requires financial institutions and nonfinancial businesses or professions, including casinos, real estate agencies, precious metals and stones dealers, and legal professionals and accountants, to file suspicious transaction reports (STRs). Section 42 of the bill requires institutions to monitor all transactions, pay attention to unusual patterns of transactions, and report any suspicious transaction. Over and above this, the reporting institution must file reports of all cash transactions

exceeding the equivalent of U.S. $10,000 in any currency. The bill also identifies 30 other statutes for the GOK to amend so that they will be consistent with the bill when it is passed.

This bill has a number of deficiencies. It does not mention terrorism, nor does it specifically define "offense" or "crime." The proposed legislation does not explicitly authorize the seizure of legitimate businesses used to launder money. The GOK tabled the bill in Parliament in November 2007, but Parliament never took the bill up, and it lapsed when Parliament recessed in December. The government republished and resubmitted the bill during the Tenth Parliament in 2008. This time, the bill made it through the second reading, one step from final passage, before it stalled. New parliamentary standing orders will enable this legislation to proceed from the point where parliament left it when the Eleventh Parliament reconvenes in 2009.

The CBK is the regulatory and supervisory authority for Kenya's deposit-taking institutions and has oversight for more than 50 such entities, as well as mortgage companies and other financial institutions. The Minister of Home Affairs supervises casinos, although its regulation of this sector is ineffective.

CBK regulations require deposit-taking institutions to verify the identity of new customers opening an account or conducting a transaction. The Banking Act amendment of December 2001 authorizes the CBK to disclose financial information to any monetary or financial regulatory authority within or outside Kenya. In 2002, the Kenya Bankers Association (KBA) issued guidelines requiring banks to report suspicious transactions to the CBK. These guidelines do not have the force of law, and only a handful of suspicious transactions had been reported by the end of 2008. Under the regulations, banks must maintain records of transactions over $100,000 and international transfers over $50,000, and report them to the CBK. A law enforcement agency can demand information from any financial institution, if it has obtained a court order. Some commercial banks and foreign exchange bureaus file STRs voluntarily, but they run the risk of civil litigation, as there are no adequate "safe harbor" provisions for reporting such transactions to the CBK. A 2002 court ruling that penalized a commercial bank for disclosing information to the CBK in response to a court order made banks wary of reporting suspicious transactions. These regulations do not cover nonbank financial institutions such as money remitters, casinos, or investment companies, and there is no enforcement mechanism behind the regulations.

There are 95 foreign exchange bureaus under GOK supervision. The Central Bank of Kenya Act (Cap 491) regulates foreign exchange bureaus, which are authorized dealers of currency. The CBK subsequently recognized that several bureaus violated portions of the Forex Bureau Guidelines, including dealing in third party checks and executing telegraphic transfers without CBK approval. The checks and transfers may have been used for fraud, tax evasion and money laundering. In response, the CBK's Banking Supervision Department issued Central Bank Circular No. 1 of 2005 instructing all foreign exchange bureaus to immediately cease dealing in telegraphic transfers and third party checks. These new guidelines, which fall under Section 33K of the Central Bank of Kenya Act, took effect on January 1, 2007.

A reported 800 registered, international nongovernmental organizations (NGOs) manage over $1 billion annually. International organizations operating in the conflict areas of the region—Southern Sudan, Somalia, Burundi and DRC—keep their money in Kenyan banks. The GOK requires all charitable and nonprofit organizations to register with the government and submit annual reports to the GOK's oversight body, the National Non-Governmental Organization Coordination Bureau. NGOs that do not comply with the annual reporting requirements can have their registrations revoked; however, the government rarely imposes such penalties. The GOK revoked the registration of some NGOs with Islamic links in 1998 after the bombing of the U.S. Embassy in Nairobi, only to later re-register them. The Non-Governmental Organization Coordination Bureau lacks the capacity to

monitor NGOs, and observers suspect that charities and other nonprofit organizations handling millions of dollars are filing inaccurate or no annual reports.

Kenya has little in the way of cross-border currency controls. GOK regulations require that any amount of cash above $5,000 be disclosed at the point of entry or exit for record-keeping purposes only, but this provision is rarely enforced, and authorities keep no record of cash smuggling attempts. The CBK guidelines call for currency exchange bureaus to furnish daily reports on any single foreign exchange transaction above $10,000, and on cumulative daily foreign exchange inflows and outflows above $100,000. Guidelines require that foreign exchange dealers ensure that cross-border payments have no connection to illegal financial transactions.

Recent investigations illustrate Kenya's vulnerability to money laundering, showing that criminals have been taking advantage of Kenya's inadequate AML regime for years by evading oversight and/or by reportedly paying off enforcement officials, other government officials, and politicians.. The Charterhouse Bank investigations in 2006 and 2007 revealed that the proceeds of large-scale evasion of import duties and taxes had been laundered through the banking system since at least 1999. In addition, the smuggled and/or under-invoiced goods may have also been marketed through the normal wholesale and retail sectors. Charterhouse Bank managers had conspired with depositors to evade import duties and taxes and launder the proceeds totaling approximately $500 million from 1999 to 2006. Charterhouse Bank also violated the Banking Act and the CBK's Prudential Guidelines by not properly maintaining records for foreign currency transactions. Available evidence made clear that the bank management had, on a large scale, consistently evaded and ignored normal internal controls by allowing many irregular activities to occur. Subsequent audits and investigations covering the period 1999-2006 found that Charterhouse Bank had violated the CBK's know-your-customer procedures in over 80 percent of its accounts, which were missing basic details such as the customer's name, address, ID photo, or signature cards. The bank management's continual violation of CBK prudential guideline CBK/PG/08 requirements to report suspicious transactions, and its efforts to conceal them from CBK examiners, also indicate that bank officials were complicit in these suspicious transactions. and understood AML controls. The Ministry did not renew the bank's license to operate once it expired.

There are strong indications that other Kenyan banks are involved in similar activities. Reportedly, Kenya's financial system may be laundering over $100 million each year. The GOK did not report any money laundering-related arrests, prosecutions, or convictions for 2007 or 2008. Kenya lacks the institutional capacity, investigative skill and equipment to conduct complex investigations independently. There have been no arrests or prosecutions for money laundering or terrorist financing.

Laws related to the seizure and forfeiture of drug trafficking-related assets are weak and disjointed. With the exception of intercepted drugs and narcotics, seizures of assets are rare. Kenya has no regulations to freeze or seize criminal or terrorist accounts. At present, the government entities responsible for tracing and seizing assets are the Central Bank of Kenya Banking Fraud Investigation Unit, the Kenya Police Anti-Narcotics and Anti-Terrorism Police Units, the Kenya Revenue Authority (KRA), and the Kenya Anti-Corruption Commission (KACC). To demand bank account records or to seize an account, the police must present evidence linking the deposits to a criminal violation and obtain a court warrant. This process is difficult to keep confidential, and as a result of leaks, serves to warn account holders of investigations. Account holders then move their accounts or contest the warrants.

Kenya has not criminalized the financing of terrorism as required by the United Nations Security Council Resolution (UNSCR) 1373 and the UN International Convention for the Suppression of Financing of Terrorism, to which it is a party. In April 2003, the GOK introduced the Suppression of Terrorism Bill into Parliament. After objections from some public groups that the bill unfairly targeted the Muslim community and unduly restricted civil rights, the GOK withdrew the bill. The GOK

drafted the Anti-Terrorism Bill in 2006, which contains provisions that would strengthen the GOK's ability to combat terrorism. It also revised the controversial text, but Muslim and human rights groups remained concerned that the government could use it to commit human rights violations. The GOK published the bill and submitted it to Parliament in 2007, but Parliament took no action. Following expressions of concern about the legislation from some Muslim members of Parliament, the bill, now renamed the Prevention of Organized Crime Bill, was not resubmitted to Parliament in 2008. The government has advised that the bill has been withdrawn for further consultations.

The CBK does not circulate the list of individuals and entities on the UN 1267 Sanctions Committee's consolidated list or the United States Office of Foreign Assets Control (OFAC) list of specially designated nationals to financial institutions. Instead, the CBK uses its bank inspection process to search for names of designated individuals and entities on the OFAC list. The CBK and the GOK have no authority to seize or freeze accounts without a court warrant. Kenya has no law specifically authorizing the seizure of the financial assets of terrorists.

Kenya is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. Kenya is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a Financial Action Task Force (FATF)-style regional body, and holds the Presidency for the administrative year of August 2008-August 2009. Kenya has an informal arrangement with the United States for the exchange of information relating to narcotics, terrorist financing, and other serious crime investigations, and has cooperated with the United States and the United Kingdom in such situations. Kenya ranks 147 out of 180 countries on the 2008 Transparency International Corruption Perceptions Index.

The Government of Kenya should pass and enact the proposed Proceeds of Crime and Anti-Money Laundering bill, and create an FIU. The GOK should criminalize the financing of terrorism and pass a law authorizing the government to seize the financial assets of terrorists. Kenyan authorities should take steps to ensure that NGOs, suspect charities and nonprofit organizations follow internationally recognized transparency standards and file complete and accurate annual reports. The CBK, law enforcement agencies, and the Ministry of Finance should improve coordination to enforce existing laws and regulations to combat money laundering, tax evasion, corruption, and smuggling. The Minister of Finance should revoke or refuse to renew the license of any bank found to have knowingly laundered money, and encourage the CBK to tighten its examinations and audits of banks. Kenyan law enforcement should be more proactive in investigating money laundering and related crimes, and its customs authorities should exert control over Kenya's borders.

Korea, Democratic Peoples Republic of

For decades, citizens of the Democratic People's Republic of Korea (DPRK) have been apprehended in international investigations trafficking in narcotics and other forms of criminal behavior, including passing counterfeit U.S. currency (including U.S. $100 "super notes") and trading in counterfeit products, such as cigarettes and patented pharmaceuticals such as Viagra and Cialis. There is substantial evidence that North Korean governmental entities and officials have been involved in the laundering of the proceeds of narcotics trafficking and other illicit activities and that they continue to be engaged in other illegal activities, including activities related to counterfeiting, through a number of front companies. The illegal revenue provides desperately needed foreign hard currency for the economy of the DPRK.

On October 25, 2006 the Standing Committee of the Supreme People's Assembly of the DPRK adopted a law "On the Prevention of Money Laundering." The law states the DPRK has a "consistent policy to prohibit money laundering," However, the law is significantly deficient in most important respects, and reportedly there is no evidence that it has been implemented.

On September 15, 2005, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) designated Macau-based Banco Delta Asia (BDA) as a primary money laundering concern under Section 311 of the USA PATRIOT Act and issued a proposed rule regarding the bank, citing the bank's systemic failures to safeguard against money laundering and other financial crimes. In its designation of BDA as a primary money laundering concern, FinCEN cited in the Federal Register "the involvement of North Korean Government agencies and front companies in a wide variety of illegal activities, including drug trafficking and the counterfeiting of goods and currency." Treasury finalized the Section 311 rule in March 2007, prohibiting U.S. financial institutions from opening or maintaining correspondent accounts for or on behalf of BDA. This rule remains in effect. Following the Section 311 designation of BDA, the Macau Monetary Authority (MMA) froze approximately U.S. $25 million in North Korean-related accounts at the bank. The MMA subsequently lifted the freeze on these funds following the issuance of the final rule.

The DPRK became a party to the 1988 UN Drug Convention in 2007. It is not a party to the UN Convention against Transnational Organized Crime or the UN Convention against Corruption. It has signed, but not ratified, the UN Convention for the Suppression of the Financing of Terrorism. North Korea is not a participant in any FATF-style regional body.

On October 11, 2008 the United States Government formally removed North Korea from the U.S. list of state sponsors of terrorism. The DPRK should develop a viable anti-money laundering/counterterrorist financing regime that comports with international standards.

Korea, Republic of

The Republic of Korea (ROK) is not considered an attractive location for international financial crimes or terrorist financing. Most money laundering appears to be associated with domestic criminal activity or corruption and official bribery. Laundering the proceeds from illegal game rooms, customs fraud, exploiting zero VAT rates applied to gold bars, trade-based money laundering, counterfeit goods and intellectual property rights violations are all areas of vulnerability. Criminal groups based in South Korea maintain international associations with others involved in human trafficking, contraband smuggling and related organized crime. As law enforcement authorities have gained more expertise investigating money laundering and financial crimes, they have become more cognizant of the problem.

The South Korean government has been a willing partner in the fight against financial crime, and has pursued international agreements toward that end. Forty kinds of serious crimes are predicate offences in Korea—two crimes under the Act on Special Cases Concerning the Prevention of Illegal Trafficking in Narcotics (1993) and 38 additional kinds of crimes under Proceeds of Crime Act (POCA), which was enacted in 2001 to broaden Korea's anti-money laundering regime by criminalizing the laundering of proceeds from additional offenses, including economic crimes, bribery, organized crime, and illegal capital flight. In addition, the concealment and disguise of property owned legally for the purpose of tax evasion, illegal refunds, customs evasion or smuggling is considered to be money laundering for the purposes of reporting of suspicious transaction reports (STRs) to KoFIU. The POCA provides for imprisonment and/or a fine for anyone receiving, disguising, or disposing of criminal funds, and also provides for confiscation and forfeiture of illegal proceeds. Financial institutions are required to report transactions known to be connected to narcotics trafficking to the Public Prosecutor's Office.

In Korea, financial institutions are required to conduct customer due diligence (CDD) under the Act on Real Name Financial Transactions and Guarantee of Secrecy ("Real Name Financial Transaction Act") (effective 1993) and the Financial Transaction Reports Act (effective January 2006), as amended (effective December 22, 2008). The Real Name Financial Transaction Act effectively prohibits anonymous accounts and accounts in obviously fictitious names and requires financial

institutions to identify and verify the identify of their customers, while the Financial Transaction Reports Act requires financial institutions to conduct CDD and to report suspicious transactions to the Korea Financial Intelligence Unit (KoFIU).

The Financial Transaction Reports Act also requires financial institutions to file suspicious transaction reports (STRs) with the Korea Financial Intelligence Unit (KoFIU). A cash transaction reports (CTR) system was implemented in January 2006. The initial threshold of KRW 50 million (U.S. $43,067) was lowered to KRW 30 million (U.S. $25,840) in January 2008 and will be further reduced to KRW 20 million (U.S. $17,227) in January 2010. The STR system was strengthened in 2004 with the introduction of a new online electronic reporting system and the lowering of the mandatory STR threshold from 50 to 20 million won. Reporting entities may file STRs for transactions below this threshold.

Money laundering controls are applied to banking and nonbank financial institutions, such as exchange houses, stock brokerages, casinos, insurance companies, merchant banks, mutual savings banks, finance companies, credit unions, credit cooperatives, trust companies, and securities companies. To strengthen Korea's AML/CTF regime, the Financial Transaction Reporting Act was amended in December 2007 (effective December 22, 2008) to establish risk-based enhanced CDD requirements; criminalize terrorist financing and establish STR obligations regarding terrorist financing; and impose AML/CTF obligations on designated nonfinancial businesses and professionals. CDD requires financial institutions to identify and verify customer identification data, including address and telephone numbers when opening an account or conducting occasional transactions of 20 million won or more. After the December 22, 2008 effective date of the Financial Transaction Reports Act amendments, KoFIU plans to expand the obligation to intermediaries, such as lawyers, accountants, or broker/dealers, not previously covered by Korea's money laundering controls. Any traveler entering Korea carrying more than $10,000 (or the equivalent in other foreign currency) is required to report the currency to the Korea Customs Service.

KoFIU was established in 2001 pursuant to the Financial Transaction Reports Act and its Presidential Enforcement Decree within the Ministry of Finance and Economy (MOFE), but was transferred in February 2008 to the Financial Services Commission (FSC). It is comprised of experts from various agencies, including the Ministry of Strategy and Finance, the Justice Ministry, the Financial Services Commission, the Bank of Korea, the National Tax Service, the National Police Agency, and the Korea Customs Service, and its independence and autonomy are guaranteed by law. It analyzes suspicious transaction reports (STRs) and currency transaction reports (CTRs), and forwards information deemed to require further investigation to appropriate law enforcement and other agencies, including the Public Prosecutor's Office (PPO); the National Police Agency; National Tax Service; Korea Customs Service; Financial Services Commission (FSC); and the National Election Commission. KoFIU also exchanges information with foreign FIUs.

In addition to receiving, analyzing and disseminating STRs and CTRs, KoFIU supervises and inspects the implementation of internal reporting systems established by financial institutions, and is responsible for coordinating the efforts of other government bodies. Officials charged with investigating money laundering and financial crimes are beginning to widen their scope to include crimes related to commodities trading and industrial smuggling, and continue to search for possible links between domestic illegal activities and international terrorist activity. In 2007, KoFIU upgraded its anti-money-laundering monitoring system by introducing the Korea Financial Intelligence System, based on scoring and data mining methods. KoFIU also encourages financial institutions, including small-scale credit unions and cooperatives, to adopt a risk-based due diligence system, focusing on types of customers and transactions, by offering those institutions training programs, and conducts education and training on financial institutions' AML/CTF obligations.

Improper disclosure of financial reports is punishable by up to five years imprisonment and a fine of up to 30 million won. The Real Name Financial Transaction and Guarantee of Secrecy Act requires that, apart from judicial requests for information, persons working in financial institutions are not to provide or reveal to others any information or data on the contents of financial transactions without receiving a written request or consent from the parties involved. However, secrecy laws do not apply when such information must be provided for submission to a court or as a result of a warrant issued by the judiciary.

South Korea joined the international community's fight against terrorism finance through enactment of the Prohibition of Financing for Offenses of Public Intimidation Act in December 2007. The Act took effect in December 2008 and is intended to implement the UN Convention for the Suppression of the Financing of Terrorism, to which South Korea has been a party since 2004. Under the Act, funds for public intimidation offenses are identified as, "any funds or assets collected, provided, delivered, or kept for use in any of the following acts committed with the intention to intimidate the public or to interfere with the exercise of rights of a national, local, or foreign government." An amendment expanding the ROKG's ability to confiscate funds related to terrorism was also submitted to the National Assembly in November 2008. The amendment adds the Prohibition act to the list of laws covered under POCA. As a result, the ROKG will not only be able to confiscate the direct proceeds of terrorism but also funds and assets (e.g. stocks and bonds) derived from those proceeds.

South Korea's Financial Services Commission may designate an individual or a group when it is necessary to prevent offenses in order to implement a generally accepted international law or an international treaty Korea is a party to, or when prevention contributes to international efforts to maintain global peace and security. The new CTF legislation is subject to the same excessively high thresholds that apply to reporting all types of suspicious activity, and also lacks requirements to identify actual beneficiaries of transactions. It is unclear whether it criminalizes the sole raising of terrorist funds.

Korea implemented regulations on October 9, 2001, to freeze financial assets of Taliban-related authorities designated by the UN Security Council. The government then revised the regulations, agreeing to list immediately all U.S. Government-requested terrorist designations under U.S. Executive Order 13224 of December 12, 2002. KoFIU circulates to its financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list, the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224, and those listed by the European Union under relevant authorities. No listed terrorist-related accounts have been reported in Korea. However, since 2003, Korea has detained or deported more than 70 people suspected of having ties to international terrorist networks.

Korean government authorities continue to investigate the underground "hawala" system, used primarily to send illegal remittances abroad by South Korea's approximately 30,000 documented foreign workers from the Middle East, as well as thousands of undocumented foreign workers (mainly ethnic Koreans from Mongolia, Uzbekistan, and Russia). Currently, gamblers who bet abroad often use alternative remittance and payment systems; however, government authorities have criminalized those activities through the Foreign Exchange Regulation Act and other laws. According to an October 2007 report by the Korea Customs Service, there were 1,311 investigations into underground remittances amounting to 2.2 trillion Won (approximately $1.84 billion) in 2003, 1,917 cases totaling 3.66 trillion Won (approximately $3.2 billion) in 2004, 1,901 cases worth 3.56 trillion Won (approximately $3.47 billion) in 2005, and 1,924 cases totaling 2.7 trillion Won (approximately $2.8 billion) in 2006. A similar report by the Korea Customs Service is not available for 2008. However, according to statistics provided by the Customs Service, there were 2,364 cases in 2007 totaling 2.39 trillion Won (approximately $2.57 billion) and 1,890 cases totaling 2.7 trillion Won (approximately $2.51 billion) from January through October 2008. Through 2004, the majority of early underground remittance cases related to the U.S. Between 2005 and June 2007, the bulk of cases involved China

(35.4 percent, approximately $2.87 billion), followed by Japan (34.9 percent, approximately $2.83 billion) and the U.S. (18 percent, $1.46 billion). Through the first ten months of 2008, China's portion of underground remittance cases remained largest (47.6 percent, approximately $1.72 billion), followed by Japan (18.6 percent, approximately $27.4 million), and the U.S. (8.3 percent, approximately $158.3 million). Although Japan accounted for more than twice as many cases as the U.S., its transactions amounted to only 17 percent of the dollar value of U.S. cases.

South Korea actively cooperates with the United States and other countries to trace and seize assets. The Anti-Public Corruption Forfeiture Act of 1994 provides for the forfeiture of the proceeds of assets derived from corruption. In November 2001, Korea established a system for identifying, tracing, freezing, seizing, and forfeiting narcotics-related and/or other assets of serious crimes. Under the system, KoFIU is responsible for analyzing and providing information on STRs that require further investigation. The Bank Account Tracing Team under the Narcotics Investigation Department of the Seoul District Prosecutor's Office (established in April 2002) is responsible for tracing and seizing drug-related assets. The Korean Government established six additional bank account tracking teams in 2004 to serve in the metropolitan cities of Busan, Daegu, Kwangju, Incheon, Daejon, and Ulsan to expand its reach. Its legal framework does not allow civil forfeiture.

Korea continues to address the problem of the transportation of counterfeit international currency. The Bank of Korea reported that through September 2008, there were 1,191 counterfeit bills found by South Korean banks worth $224,000. The 2008 dollar amount represents a 79 percent decrease from the same period in 2007. Bank experts confirm that the amount of forged U.S. currency is on a decline.

South Korea has a number of free economic zones (FEZs) that enjoy certain tax privileges. However, companies operating within them are subject to the same general laws on financial transactions as companies operating elsewhere, and reportedly there is no indication these FEZs are being used in trade-based money laundering schemes or for terrorist financing. Korea mandates extensive entrance screening to determine companies' eligibility to participate in FEZ areas, and firms are subject to standard disclosure rules and criminal laws. In 2007 Korea had seven FEZs, as a result of the June 2004 re-categorization of the three port cities of Busan, Incheon, and Kwangyang as FEZs. They were re-categorized from their previous designation of "customs-free areas" to avoid confusion from the earlier dual system of production-focused FEZs, and logistics-oriented "customs-free zones." Incheon International Airport has been incorporated into the FEZs.

Korea is a party to the 1988 UN Drug Convention, the UN Convention for Suppression of the Financing of Terrorism in December and the UN Convention against Corruption, but is not a party to the UN Convention against Transnational Organized Crime. Korea is an active member of the Asia/Pacific Group on Money Laundering (APG) and its FIU became a member of the Egmont Group in 2002. An extradition treaty between the United States and the ROK entered into force in December 1999. The United States and the ROK cooperate in judicial matters under a Mutual Legal Assistance Treaty, which entered into force in 1997. In addition, the FIU continues to actively pursue information-sharing agreements with a number of countries, and had signed memoranda of understanding with 36 countries. Korea became an observer to the Financial Action Task Force (FATF) in July 2006 and is working to complete the accession process and obtain full membership.

Among other priorities, the government should extend its anti-money laundering regime to intermediaries such as lawyers, accountants, broker/dealers and informal lending widely recognized as potential blind spots. Korea should eliminate the high monetary threshold for reporting suspicious transactions and extend the reporting obligation to attempted transactions. The Republic of Korea should continue its policy of active participation in international anti-money laundering efforts, both bilaterally and in multilateral fora. Spurred by enhanced local and international concern, Korean law enforcement officials and policymakers now understand the potential negative impact of such activity on their country, and have begun to take steps to combat its growth. The ROKG efforts will become

increasingly important due to the continued growth and greater integration of Korea's financial sector into the world economy. The ROKG should become a party to the UN Convention against Transnational Organized Crime.

Kuwait

Despite its geographic location in the Gulf region, money laundering is not believed to be a significant problem in Kuwait. Illicit funds reportedly are generated largely as revenues from drug and alcohol smuggling into the country and the sale of counterfeit goods. The potential for the financing of terrorism through the misuse of charities continues to be a major concern.

Kuwait has ten private local commercial banks, including three Islamic banks; the Kuwait Finance House (KFH), Boubyan Islamic Bank, and Kuwait International Bank, all of which provide conventional banking services comparable to Western-style commercial banks. Kuwait also has one specialized bank, Industrial Bank of Kuwait, a government-owned bank that provides medium and long-term financing. On June 11, 2008 the Central Bank of Kuwait (CBK) authorized the Bank of Kuwait and the Middle East (BKME) to become an Islamic bank, which will increase the number of Islamic banks in Kuwait to four. The Commercial Bank of Kuwait has filed an application to convert to an Islamic bank. Legislation to launch another Islamic bank is pending in Parliament. The bank will be approximately 50 percent owned by the Government of Kuwait (GOK). These additions demonstrate the rapid growth of Islamic banking in Kuwait.

The Kuwaiti banking sector opened to foreign competition under Kuwait's 2001 Foreign Direct Investment Law, which enabled foreigners to own up to 49 percent of existing or newly formed Kuwaiti banks, subject to approval by the CBK. In January 2004, the National Assembly gave final approval to a bill permitting 100 percent foreign ownership of banks. However, foreign-owned banks which are restricted to opening only one branch can only offer investment banking services and are prohibited from competing in the retail banking sector. In August 2004, BNP Paribas was the first foreign bank granted a license to operate in Kuwait, followed by HSBC in October 2005, Citibank in late 2006, Abu Dhabi National Bank and Qatar National Bank in 2007, and Doha Bank in 2008. Gulf Bank, Kuwait's second largest lender, sought assistance from the Central Bank of Kuwait in October 2008 after a client defaulted on approximately $1.4 billion of liabilities related to euro-dollar derivatives contracts. On November 20, Gulf Bank announced a recapitalization plan, giving priority to existing shareholders, but with the government controlled Kuwait Investment Authority serving as buyer of last resort. The crisis at Gulf Bank prompted the Parliament to enact legislation guaranteeing all deposits in all banks operating in Kuwait. CBK recently approved an additional three foreign banks to open branches in Kuwait, Al-Mashreq Bank, Al-Rajhi Bank and Bank of Muscat.

On March 10, 2002, the Emir of Kuwait (Head of State) signed Law No. 35, which criminalized money laundering. Law No. 35 does not specifically cite terrorist financing as a crime. The law stipulates that banks and financial institutions may not keep or open anonymous accounts or accounts in fictitious or symbolic names, and that banks must require proper identification of both regular and occasional clients. The law also requires banks to keep all records of transactions and customer identification information for a minimum of five years, conduct anti-money laundering and terrorist financing training to all levels of employees, and establish proper internal control systems.

Law No. 35 requires banks to file suspicious transactions reports (STRs) to the Office of Public Prosecution (OPP), which in turn will refer reports of suspicious transactions to the CBK for analysis. The anti-money laundering law provides for a penalty of up to seven years' imprisonment in addition to fines and asset confiscation. The penalty is doubled if an organized group commits the crime, or if the offender took advantage of his influence or his professional position. Moreover, banks and financial institutions may face a steep fine (approximately $3.3 million) if found in violation of the law.

The law includes articles on international cooperation and the monitoring of cash and precious metals transactions. Currency smuggling into Kuwait is criminalized under Law No. 35, although cash reporting requirements are not uniformly enforced at ports of entry (except at Kuwait International Airport and Al-Abdali Border Exit). Provisions of Article 4 of Law No. 35 require travelers to disclose any national or foreign currency, gold bullion, or other precious materials in their possession valued in excess of 3,000 Kuwaiti dinars (approximately $10,900) to customs authorities, upon entering the country. However, the law does not require individuals to file declaration forms when carrying cash or precious metals out of Kuwait. There has only been one case of currency smuggling reported in 2008, which has not gone to court. The case reportedly involved smuggling of counterfeit U.S. dollar bills, Euros and GCC currencies.

The National Committee for Anti-Money Laundering and the Combating of Terrorist Financing is responsible for administering Kuwait's anti-money laundering/combating terrorist financing (AML/CTF) regime. In April 2004, the Ministry of Finance issued Ministerial Decision No. 11 (MD No. 11/224), which transferred the chairmanship of the National Committee, formerly headed by the Minister of Finance, to the Governor of the Central Bank of Kuwait. The Committee is comprised of representatives from the Ministries of Interior, Foreign Affairs, Commerce and Industry, Finance, and Labor and Social Affairs; the Office of Public Prosecution, the Kuwait Stock Exchange, the General Customs Authority, the Union of Kuwaiti Banks, and the Central Bank.

The National Committee is mandated with drawing up the country's strategy and policy with regard to anti-money laundering and terrorist financing; drafting the necessary legislation and amendments to Law No. 35, along with pertinent regulations; coordinating between the concerned ministries and agencies; following up on domestic, regional, and international developments and making needed recommendations; setting up appropriate channels of communication with regional and international institutions and organizations; and representing Kuwait in domestic, regional, and international meetings and conferences. In addition, the Chairman is entrusted with issuing regulations and procedures that he deems appropriate for the Committee's duties, responsibilities, and organization of its activities.

Kuwait, however, has been unable to implement fully its current anti-money laundering law due in part to structural inconsistencies within the law itself. Kuwait's Financial Intelligence Unit (FIU) is not an independent body in accordance with the current international standards, but rather is under the direct supervision of the Central Bank of Kuwait. In addition, vague delineations of the roles and responsibilities of the government entities involved continue to hinder the overall effectiveness of Kuwait's anti-money laundering regime. Cognizant of these shortcomings, the National Committee drafted a revision of Law No. 35 that would bring Kuwait into compliance with international standards, and would criminalize terrorist financing. According to Kuwaiti officials, the draft law was referred to the Council of Ministers on August 18, 2008 and is still pending cabinet approval and submission to Kuwait's National Assembly for ratification.

In addition to Law No. 35, anti-money laundering reporting requirements and other rules are contained in CBK instructions No. (2/sb/92/2002), which took effect on December 1, 2002, superseding instructions No. (2/sb/50/97). The revised instructions provide for, *inter alia*, customer identification and the prohibition of anonymous or fictitious accounts (Articles 1-5); the requirement to keep records of all banking transactions for five years (Article 7); electronic transactions (Article 8); the requirement to investigate transactions that are unusually large or have no apparent economic or lawful purpose (Article 10); the requirement to establish internal controls and policies to combat money laundering and terrorism finance, including the establishment of internal units to oversee compliance with relevant regulations (Article 14 and 15); and the requirement to report to the Central Bank all cash transactions in excess of approximately $10,000 (Article 20). In addition, the Central Bank distributed detailed instructions and guidelines to help bank employees identify suspicious transactions. At the Central Bank's instructions, banks are no longer required to block assets for 48

hours on suspected accounts in an effort to avoid "tipping off" suspected accountholders. The CBK, upon notification from the Ministry of Foreign Affairs (MFA), issues circulars to units subject to supervision requiring them to freeze the assets of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list. Financial entities are instructed to freeze any such assets immediately and for an indefinite period of time, pending further instructions from the Central Bank, which in turn receives its designation guidance from the MFA.

On June 23, 2003, the CBK issued Resolution No. 1/191/2003, establishing the Kuwaiti Financial Inquiries Unit (KFIU) within the Central Bank, which would act as Kuwait's FIU. The KFIU is comprised of seven part-time CBK staff and headed by the Central Bank Governor. The responsibilities of the FIU are to receive and analyze reports of suspected money laundering activities from the OPP, establish a database of suspicious transactions, conduct anti-money laundering training and carry out domestic and international exchanges of information in cooperation with the OPP. Although the Unit should act as the country's financial intelligence unit, Law No. 35/2002 did not mandate the KFIU to act as the central or sole unit for the receipt, analysis, and dissemination of STRs; Banks in Kuwait are required to file STRs with the OPP, rather than directly with the FIU. However, based on an MOU with the Central Bank, STRs are referred from the OPP to the FIU for financial analysis. The FIU conducts analysis and reports any findings to the OPP for the initiation of a criminal case, if necessary. The FIU's access to information is limited, due to its inability to share information abroad without prior approval from the OPP. Kuwaiti officials agree that the current limits on information sharing by the FIU will have to be addressed by amending the law, which was revised by the National Committee in 2006 and is currently under governmental review. The KFIU is not a member of the Egmont Group.

There are about 148 money exchange businesses (MEBs) operating in Kuwait that are authorized to exchange foreign currency only. None of these MEBs are formal financial institutions, and therefore are under the supervision of the Ministry of Commerce and Industry (MOCI) rather than the Central Bank. The CBK has reached an agreement that tasks the MOCI with the enforcement of all anti-money laundering (AML) laws and regulations in supervising such businesses. MOCI is working to encourage MEBs to apply for and obtain company licenses, and to register with the CBK.

The MOCI's Office of Combating Money Laundering Operations was established in 2003, and supervises approximately 2,500 insurance agents, brokers and companies; investment companies; exchange bureaus; jewelry establishments (including gold, metal and other precious commodity traders); brokers in the Kuwait Stock Exchange; and other financial brokers. All new companies seeking a business license are required to receive AML awareness training from the MOCI before a license is granted. These firms must abide by all regulations concerning customer identification, record keeping of all transactions for five years, establishment of internal control systems, and the reporting of suspicious transactions. MOCI conducts both mandatory follow-up visits and unannounced inspections to ensure continued compliance. Businesses that are found to be in violation of the provisions of Law No. 35/2002 receive an official warning from MOCI for the first offense. The second and third violations result in closure for two weeks and one month respectively. The fourth violation results in revocation of the license and closure of the business. Reportedly, 14 exchange houses were closed in 2007-2008 for violating MOCI's instructions, and two cases were referred to the Public Prosecutor's Office for violation of customer contracts.

In August 2002, the Kuwaiti Ministry of Social Affairs and Labor (MOSAL) issued a ministerial decree creating the Department of Charitable Organizations (DCO). The primary responsibilities of the new department are to receive applications for registration from charitable organizations, monitor their operations, and establish a new accounting system to ensure that such organizations comply with the law both at home and abroad. The DCO has established guidelines for charities explaining donation collection procedures and regulating financial activities. The DCO is also charged with conducting periodic inspections to ensure that charities maintain administrative, accounting, and organizational

standards according to Kuwaiti law. The DCO mandates the certification of charities' financial activities by external auditors, and limits the ability to transfer funds abroad only to select charities approved by MOSAL. There are currently 10 charities approved by MOSAL. MOSAL also requires all transfers of funds abroad to be made between authorized charity officials. MFA reportedly monitors all transactions funneled to charities abroad. Banks and money exchange businesses (MEBs) are not allowed to transfer any charitable funds outside of Kuwait without prior permission from MOSAL. In addition, any such wire transactions must be reported to the CBK, which maintains a monthly database of all transactions conducted by charities. Despite these restrictions, in June 2008, the U.S. Department of the Treasury designated the Kuwait-based Revival of Islamic Heritage Society (RIHS) for providing financial and material support to al Qaida and al Qaida affiliates, including Lashkar e-Tayyiba, Jemaah Islamiyah, and Al-Itihaad al-Islamiya and for providing financial support for acts of terrorism.

Unauthorized public donations, including Zakat (alms) collections in mosques, are also prohibited except during the Islamic holy month of Ramadan. The donations are supervised by MOSAL. In 2005, the MOSAL introduced a pilot program requiring charities to raise donations through the sale of government-provided coupons during Ramadan. MOSAL continued this program in 2006 and in 2007 implemented the collection of donations through a voucher system and electronic bank transfers. The GOK plans to encourage the electronic collection of charitable funds using a combination of electronic kiosks, hand-held collection machines, and text messaging are being reviewed by the Legal Committee at the Cabinet Council and expected to be approved soon. Such devices would generate an electronic record of the funds collected, which will then be subject to MOSAL supervision.

Kuwait is a member of the Gulf Cooperation Council (GCC), which is itself a member of the Financial Action Task Force (FATF). In addition, it is a member of the Middle East and North Africa Financial Action Task Force (MENAFATF). Kuwait has played an active role in the MENAFATF, particularly through its participation in drafting regulations and guidelines pertaining to charities oversight and cash couriers.

Kuwait is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. It is not a party to the UN Convention for the Suppression of the Financing of Terrorism. Kuwait and the United States do not have a mutual legal assistance agreement.

The Government of Kuwait should significantly accelerate its ongoing efforts to revise Law No. 35/2002 to criminalize terrorist financing; strengthen charity oversight, especially in its overseas operations; develop an independent FIU that meets international standards including the sharing of information with foreign FIUs; and improve international information sharing, as well as sharing between the government and financial institutions. More interagency cooperation and coordination between the Kuwaiti Financial Intelligence Unit and other concerned parties could yield significant improvements in proactive investigations and international information exchange. The Kuwaiti Financial Inquiries Unit should be able to independently share financial information with its foreign counterparts, and receive, analyze and disseminate suspicious transaction reports without obtaining prior authorization from the Office of the Public Prosecutor. Pursuant to FATF Special Recommendation IX, Kuwait should implement and enforce a uniform cash declaration policy for inbound and outbound travelers for all its ports. There are minimal money laundering investigations and prosecutions in Kuwait. Similar to many other countries in the Gulf, Kuwait primarily relies too heavily on STRs to initiate money laundering investigations. Rather, Kuwaiti law enforcement and customs authorities should be more active in identifying suspect behavior that could be indicative of money laundering during their routine investigations of predicate offenses. Enhanced training for most sectors involved in Kuwait's anti-money laundering efforts is required. Kuwait should become a party to the UN Convention for the Suppression of the Financing of Terrorism.

Laos

Laos is neither an important regional financial center, nor an offshore financial center. Although the extent of the money laundering risks are unknown, illegal timber sales, corruption, cross-border smuggling of goods, illicit proceeds from the sale of methamphetamine (ATS) known locally as "ya ba" (crazy medicine), and domestic crime can be sources of laundered funds. There are continued reports of illicit funds being diverted into some hotel construction, resort development, and industrial tree cropping projects. Anecdotal evidence indicates that large cash deposits related to illicit activities are generally made across the border in Thailand, or perhaps in China.

The Lao banking sector is dominated by state-owned commercial banks in need of continued reform. Although some foreign banks have branches in Laos, the classic "offshore" banking is not permitted. In 2008 three new private commercial banks became operational, including the ANZV Bank, an Australian-Lao joint venture arising from Australia-based ANZ's purchase of the Vientiane Commercial Bank. The small scale and poor financial condition of Lao banks may make them more likely venues for certain kinds of illicit transactions. These banks are not optimal for moving large amounts of money in any single transaction, due to the visibility of such movements in the existing small-scale, low-tech environment. Reportedly, there has been no notable increase in financial crimes. There have been no money laundering investigations initiated to date. There is smuggling of consumer goods across the Mekong and in areas near the Chinese border in the north, which could be associated with trade-based money laundering. This smuggling activity is an easy way to avoid paying customs duties and the inconvenience of undergoing weigh station inspections near the Lao and Chinese borders. There are two special economic zones in Savannakhet Province, one each near the Thai and Vietnamese borders on the recently opened Danang-Mukdahan (Thailand) highway. Both are awaiting tenants and there is no indication they are currently used to launder money or finance terrorism. China has leased a similar special economic zone in Luang Namtha Province on the China-Thailand highway at Boten. Within the zone is a casino that potentially could be utilized to launder funds, though there is no evidence that the gaming facility is currently being employed for that purpose. At least two other major new casinos are under construction as 2008, one in the northern province of Bokeo (Chinese financed) and one in the southern province of Savannakhet (Macao financed). There are reports that more casinos are on the way. All foreign investment in Laos must first be approved by the government's Ministry of Planning and Investment, which provides due diligence on companies seeking to invest in Laos. Due to general poverty, lack of human capacity, and weak governance, the ability to successfully discover companies bent on illicit transactions is suspect.

Money laundering is a criminal offense in Laos and anti-money laundering measures are included in at least two separate decrees. The penal code contains a provision adopted in November 2005 (Article 64) that criminalizes money laundering and provides sentencing guidelines. On March 27, 2006, the Prime Minister issued a detailed decree, No. 55/PM, on anti-money laundering, based on a model law provided by the Asian Development Bank. Because of the unique nature of Lao governance, the decree is roughly equivalent to a law, but it is much easier to change than a law passed by the National Assembly. However, the decrees don't have the same legal effect as provisions in the penal code. One Annex of the decree lists predicate offences for money laundering in relation to all crimes with a prison sentence of a year or more. In addition, the decree specifically lists the following predicate offences as serious offences with respect to money laundering: terrorism, financing of terrorism, human trafficking and smuggling; sexual exploitation, human exportation or illegal migration, the production, sales, and possession of narcotic drugs, illicit arms and dynamite trafficking; concealment and trafficking of people's property, corruption, the receipt and giving of bribes, swindling, embezzlement, robbery, property theft; counterfeiting money and its use; murder and grievous bodily injury, illegal apprehension and detention, violation of state tax rules and regulations, extortion, as well as check forgery and the illicit use of false checks, bonds, and other financial instruments. The

GOL is still considering drafting an AML law in order to create a comprehensive AML regime in line with the international standards established by the FATF.

A revision to the penal law in November 2005 includes Article 58/2 which makes financing terrorism punishable by fines of 10 to 50 million Kip (approximately $1,7,000-$5,800), prison sentences from 10 to 20 years, and the possibility of the death penalty. The Bank of Laos has circulated lists of individuals and entities on the UN 1267 sanctions coordinated list.

The Anti-Money Laundering Intelligence Unit (AMLIU) was formally established as a unit within the Bank of Laos on May 14, 2007, replacing the previous ad hoc Pre-Financial Intelligence Unit (FIU). According to the GOL report presented at the July 2007 Asia-Pacific Group plenary, the AMLIU Director and staff "have an action plan to develop full functionality of the AMLIU and to implement provisions of the Decree on Prevention of Money Laundering." This Action Plan was finalized by the AMLIU in 2008. Furthermore, the Bank of Lao established a national fourteen member AML Working Group in 2008, composed of representatives of key GOL ministries and agencies, including Ministry of Defense, Ministry of Finance, Ministry of Public Security, Ministry of Industry and Commerce, Prime Minister's Office, Office of the Supreme Peoples' Court and the Government Inspection Committee, to improve communications and coordination on AML issues within Laos. It is currently beginning a process to set up a National Coordinating Committee that will provide a mechanism for coordination and policy development at a senior level within government The AMLIU, which has a staff of eight, acts as an FIU and supervises financial institutions for their compliance with anti-money laundering decrees and regulations. The AMLIU has no criminal investigative responsibilities, nor does it have any agreements with other FIUs. It does not yet have the technology to store and analyze financial reports or to provide for electronic reporting by banks. The AMLIU created a five part, 48-question suspicious transaction report (STR) form and distributed it to all banks along with guidance on October 15, 2007. The AMLIU followed up with the commercial banks in 2008 with a series of meetings to review these regulations. Banks are required to report suspicious transactions (STRs), of which 10 were reported in 2008, although there were no arrests for terrorist financing or money laundering.

The guidance issued by the AMLIU related to suspicious transactions, Bank of Lao No. 66/AMLIU, dated October 15, 2007, and does not contain any thresholds for reporting STRs. Instead, it requires financial institutions to take into account a wide range of factors that could indicate an illegal transaction. The decree on AML requires any transaction over $10,000 to be reported by banks and others to AMLIU but in practice no large cash reporting is taking place due to the lack of technology. Reporting officers are protected against any suit or action related to the reporting process. While the 2006 decree on ant-money laundering specifically applies to nonbank financial institutions (NBFI), the AMLIU is currently working only with commercial banks as it implements the STR form. It will expand its oversight once the necessary agreements with other supervising agencies are in place. Effective adoption of the STR and cash reporting system is likely to take a number of years. Cultural norms are such that it is unlikely that banks and NBFIs will soon begin generating reports related to customers perceived as being either influential, politically powerful, or coming from prominent families. However, the 10 STRs received by the AMLIU in 2008 represent a modest beginning. On September 16 2008 the BOL issued Guideline No. 02/BOL on 'AML Procedures and Operational Controls of Reporting Institutions under Supervision of the Bank of Lao' to give clarity to banks and other reporting institutions on their responsibilities and obligations on prevention of money laundering.

Lao law restricts the export of the national currency, the kip, limiting residents and nonresidents to 5,000,000 kip per trip (approximately $500.) Larger amounts may be approved by the Bank of Laos. It is likely that the currency restrictions and undeveloped banking sector encourage the use of alternative remittance systems. When carrying cash across international borders, Laos requires a declaration for amounts over $5,000 when brought into the country and when being taken out. Failure to show a

declaration of incoming cash when exporting it could lead to seizure of the money or a fine. As customs procedures in Laos are undeveloped and open to corruption, enforcing this decree will require political will, development of a professional customs service, compensation reform, further training, and increased capital investments. The Prime Minister's decree on money laundering provides for application of deterring measures, including freezing and confiscation of assets subject to appropriate laws and regulations specifically. The authority is broadly worded. It is not clear which government authority has responsibility for asset seizures, although indications are that the Prosecutor's Office would take the lead. The GOL continues to build a framework of law and institutions; however, at this stage of development, enforcement of enacted legislation and decrees is weak. No legal asset seizures related to narcotics trafficking or terrorism were reported in 2008. A considerable number of assets are reportedly seized by police counternarcotics units from suspected drug traffickers, but these assets usually remain in the custody of the police. However, the new "Law on Drugs and Article 146 of the Penal Code" promulgated in early 2008 does now allow for the seizure of assets from drug traffickers (Article 35) but the procedures for actually selling such assets and accounting for the funds have yet to be developed or implemented. Currently, most such assets remain under police custody.

Laos' decree on money laundering authorizes the government to cooperate with foreign governments to deter money laundering of any sort, with caveats for the protection of national security and sovereignty. There are no specific agreements with the United States relating to the exchange of information on money laundering. The Bank of Lao has coordinated with the Embassy on a number of cases related to counterfeit U.S. currency.

The GOL is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime and became a party to the UN Convention for the Suppression of Financing of Terrorism in September. The GOL participates in Association of Southeast Asian Nations (ASEAN) regional conferences on money laundering. Laos moved from observer status to membership in the Asia Pacific Group on Money Laundering. (APG) during the July, 2007 annual plenary in Perth, Australia and attended the 2008 plenary in Bali, Indonesia.

In order to comport with international standards, the GOL should enact comprehensive anti-money laundering/counterterrorist financing legislation, as decrees are not recognized by international organizations as having the force of law. Such legislation would include, but not be limited to the promulgation of implementing regulations, strengthening of the nascent financial intelligence unit, an increase in the number and type of obligated entities, a prohibition against "tipping off", safe harbor provisions for those reporting suspicious financial transactions to the FIU, criminal penalties for opening or operating false name accounts and for structuring cash transactions to avoid the cash reporting threshold. Guidance to all reporting entities and the issuance of AML policy, procedure, and operational controls for banks should be issued and the GOL should encourage further development of domestic AML coordination mechanisms. The GOL should also fully implement the UN Convention on Transnational Organized Crime and become a party to the UN Convention against Corruption.

Latvia

Latvia is a growing regional financial center that has a large number of commercial banks with a sizeable nonresident deposit base. Sources of laundered money in Latvia primarily involve tax evasion and corruption, but also include to a lesser degree counterfeiting, white-collar crime, extortion, financial/banking crimes, stolen cars, contraband smuggling, and prostitution. Some proceeds of tax evasion appear to originate from outside of Latvia. Reportedly, Russian organized crime is active in Latvia, and authorities believe that a portion of domestically obtained criminal proceeds derives from organized crime. State Narcotics Police have reportedly not found a significant link between smuggled goods on the black market and narcotics proceeds. Currency transactions involving international narcotics trafficking proceeds do not include significant amounts of United States currency and

apparently do not derive from illegal drug sales in the United States. However, U.S. law enforcement agencies have determined that some U.S criminal elements utilize the Latvian financial sector to launder narcotics proceeds. U.S. law enforcement agencies continue to cooperate with Latvian counterparts on matters of money laundering and affiliated crimes. As Latvia's banking controls tighten, regulators report a pattern of certain accounts moving to other banks in the region and assert that alleged criminal activity is moving to places where it is easier to conduct business. However, there is insufficient data available for United States authorities to assess this claim.

Latvia is not an offshore financial center, although four special economic zones exist in Latvia providing a variety of significant tax incentives for the manufacturing, outsourcing, logistics centers, and transshipment of goods to other free trade zones. These zones are located at the free ports of Ventspils, Riga, and Liepaja, and in the inland city of Rezekne near the Russian and Belarusian borders. Though there have been instances of reported cigarette smuggling to and from warehouses in the free trade zones, there have been no confirmed cases of the zones being used for money laundering schemes or by the financiers of terrorism. Latvia's banking regulator, the Financial and Capital Market Commission (FCMC), states that the zones are covered by the same regulatory oversight and enterprise registration regulations that exist for nonzone areas.

In 2004, the Government of Latvia (GOL) criminalized money laundering for all crimes listed in the Criminal Law of the Latvian Republic. Latvia's new anti-money laundering (AML) law, The Law on Prevention of Money Laundering and Terrorist Financing, has been in force since August 2008 and Latvia updated the acts relevant to enforcement at the end of 2008.

Entities subject to the law include credit and financial institutions, tax advisors, external accountants, sworn auditors and lawyers, notaries, company service providers, real estate agents, lottery and gambling organizers and sectors listed in the European Commission directive. Other sectors not specifically indicated in this law also have a duty to comply with the requirements of AML in reporting unusual or suspicious transactions, and are also subject to legal remedies. The new law introduces a risk-based approach: entities must assess the client's risk for anti-money laundering and terrorist financing, then choose between simplified and enhanced customer due diligence. The law states that obliged entities must identify all clients, both long term and those who wish to carry out individual transactions. The identification requirement includes compulsory identification of customers who pay cash for transactions of 15,000 euros (approximately $18,800) or more.

The law requires obliged entities to gather customer identification and institutes record keeping requirements. Entities must retain transaction and identification data for at least five years after ending a business relationship with a client. Institutions engaging in financial transactions must report both suspicious activities and unusual transactions, including large cash transactions, to the financial intelligence unit (FIU). Suspicious and unusual transactions must be reported immediately. Obliged entities must also file an unusual activity report using the indicator list provided by the FIU if there appears to be laundering or attempted laundering of the proceeds from crime or terrorist financing.

Obliged entities must also report cash transactions. This requirement applies regardless of size or number of transactions. Depending on the situation and the business, the reporting threshold may vary from 1000 lats to 40,000 lats (approximately $2000-$80,000). Entities subject to the law have the ability to freeze accounts if they suspect money laundering or terrorist financing. If they find the activity of an account questionable, they may close the account on their own initiative. Negligent money laundering is illegal in Latvia and authorities can prosecute. Deliberately providing false information about a beneficial owner to a credit or financial institution is also illegal.

By establishing a framework to improve the flow of information, the new AML law removes many procedural hurdles that had stymied law enforcement agencies responsible for investigating and prosecuting financial crimes. The FIU can now share information directly with Latvian law

enforcement agencies instead of submitting it through the Prosecutor General's office. The law also authorizes the Latvian FIU to exchange information with any government.

The Council for Development of the Financial Sector (formerly the Anti-money Laundering Council) is the coordinator of AML and counterterrorist financing (CTF) issues on the state level. The Prime Minister chairs this body and it continued to meet during 2008.

Latvian legislation instituting a cross-border currency declaration requirement took effect on July 1, 2006. The law obliges all persons transporting more than 10,000 euros (approximately $12,500) in cash or monetary instruments between Latvia and any non-European Union (EU) member state, to declare the money to a customs officer, or, where there is no customs checkpoint, to a border guard. People moving within the EU are exempt from any declaration requirement. Latvian government agencies share these declarations amongst themselves.

Banks may not open accounts without conducting customer due diligence and obtaining client identification documents for both residents and nonresidents. When conducting due diligence on legal entities, banks must identify and verify the customer, establish the identity of the beneficial owner of a company, determine the reason for the opening of the account, define the expected transactions and monitor transactions as they are made. Sanctions levied against banks for noncompliance reach fines up to 100,000 lats (approximately $175,000). Latvia does not have secrecy laws that prevent the disclosure of client and ownership information to bank supervisors or law enforcement officers. Safe harbor provisions protect reporting individuals. The number and size of the nonresident accounts continues to represent a significant AML/CTF vulnerability given the inherent problems associated with establishing accounts based on non-face-to-face relationships. According to the FCMC, as of June 2008 nonresident deposits amounted to approximately $10 billion, or just under 45 percent of total deposits in Latvia.

The Bank of Latvia supervises the currency exchange sector. The FCMC serves as the GOL's unified public financial services regulator, overseeing commercial banks and nonbank financial institutions, the Riga Stock Exchange (part of OMX NASDAQ), and the insurance sector, which includes insurance companies, reinsurance companies and insurance intermediaries. The FCMC conducts regular audits of credit institutions. It also levies financial sanctions on companies that fail to file mandatory reports of unusual transactions and to those that submit incomplete or deficient information on both the economic activities of businesses, and deficiencies in internal controls of banks. The FIU also works to ensure accurate reporting by determining whether it has received corresponding suspicious transactions reports (STRs) when suspicious transactions occur between Latvian banks.

The "Regulations for Enhanced Customer Due Diligence," in force since August 2008, define when financial institutions must perform enhanced customer due diligence, the performance procedure for and the minimum extent of enhanced customer due diligence at the beginning of or during a business relationship, the categories of risk, the special measures of enhanced due diligence, and the performance procedure as it applies to customer transactions. If a customer does not meet minimum standards, a bank must terminate its relationship with that customer within 45 days of the determination. Banks must also identify customers who have no account or relationship with the bank, but wish to make transactions. The FCMC has the authority to share information with Latvian law enforcement agencies and receive data regarding potential financial crime patterns uncovered by police or prosecutors.

The Gambling and Lotteries Law outlines gaming and lottery organizers' rights and obligations in relation to preventing money laundering. Organizers have certain restrictions and must submit suspicious or unusual transaction reports to the FIU. They also must perform other AML activities as required by Latvian law. The Lottery and Gaming Supervisory Inspection Commission is currently updating Suspicious Activity Report (SAR) indicator guidelines for organizers based on technology and product changes in the gaming industry. The mutual evaluation report of Latvia (MER) conducted

by the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) and the International Monetary Fund and adopted by the MONEYVAL plenary in 2006, found compliance with the Financial Action Task Force (FATF) 40 Recommendations and Nine Special Recommendations on Terrorist Financing.

In addition to the legislative and regulatory requirements in place, the Association of Latvian Commercial Banks (ALCB) plays an active role in setting standards on AML issues for Latvian banks and actively participated in the creation of the new AML law. The ALCB has adopted regulations entitled "Prevention of Money Laundering" as guidance, as well as a "Declaration on Taking Aggressive Action against Money Laundering," which all Latvian banks signed in 2004. The ALCB has also adopted a voluntary measure, which all of the banks observe, to limit cash withdrawals from automated teller machines to 1,000 lats (approximately $1,800) per day. In 2008, the ALCB Council approved an "Action Plan to Enhance Transparency of Offshore Customers Serviced by Banks in Latvia." In addition to acting as an industry representative to government and regulator, the ACLB organizes regular education courses on AML/CTF issues for bank employees. Since 2005, 476 professionals from banks, insurance companies, leasing companies, the Latvian Post Office, business school and finance and auditing companies have been trained in Basic, Advanced or Expert certificate courses, which include a five-day extensive training program followed by an examination.

The Office for the Prevention of the Laundering of Proceeds Derived from Criminal Activity, known as the Control Service, is Latvia's FIU. Although the Control Service is part of the Latvian Prosecutor General's Office, which monitors it, its budget is separate. The Control Service is responsible for coordination, application and assessment of Latvia's AML policy and overall effectiveness. Latvia's FIU received over 34,000 reports in 2007. During the first 10 months of 2008 the Control Service received nearly 29,000 reports of suspicious and unusual financial transactions, and sent 117 cases, encompassing more than 2100 financial transactions, to law enforcement authorities.

Through the new AML law Latvia has addressed concerns described by the MER, in particular a concern regarding over-reliance on lists of either examples of suspicious transactions or indicators for unusual transactions for STR filing, as opposed to examination of actual transactions. The new AML law mandates reporting on unusual transactions and that this reporting must be analyzed by the FIU. The law does not define a list of indicators for identifying suspicious activities or filing Suspicious Activity Reports (SARs), and authorities explain the types of suspicious transactions through training. These institutions file SARs based on their analysis and findings.

Latvia has taken steps to ensure effective implementation of the new AML law by providing training to explain the intent and details to the law's subjects. Both individual financial institutions and entire sectors, such as tax consultants, have received this training. The ALCB organizes five-day seminars for this purpose, and certifies the attending staff. The ALCB provided five such trainings in 2008.

The Control Service conducts a preliminary analysis of the suspicious and unusual reports. It may then forward the information to law enforcement authorities that investigate money laundering and other criminal cases. The Control Service can disseminate case information to a specialized Anti-Money Laundering Investigation Unit of the Economic Police within the State Police, as well as to the Financial Police (under the State Revenue Service of the Ministry of Finance); the Bureau for the Prevention and Combat of Corruption (Anti-Corruption Bureau, KNAB) for crimes committed by public officials; the Security Police (for cases concerning terrorism and terrorist financing); and other law enforcement authorities.

The Control Service has access to all state and municipal databases. It does not have direct access to the databases of financial institutions, but requests data as needed. The Control Service shares information with other FIUs and has cooperation agreements on information exchange with FIUs in eighteen countries. The Control Service is a member of the Egmont Group of financial intelligence units. The FIU has the power to suspend debit operations in an account if it believes that any crime,

including terrorist financing or money laundering, has been attempted or committed. If a bank exercises its right to refrain from executing a transaction and reports this to the FIU, it is then the FIU's decision whether to freeze the assets for 60 days or to allow the transaction to proceed. If the FIU issues a freezing order, it must forward the case to law enforcement or the Prosecutor's Office within 10 business days.

In 2007 the Latvian FIU issued 94 freezing orders for the total amount of 6,5 million lats (approximately $11.4 million). In the first 10 months of 2008 the FIU issued 75 orders to freeze assets, with a total of over 1.5 million lats (approximately $2.6 million). Latvia's FIU reports that cooperation from the banking community in tracing and freezing assets has been excellent.

The adoption of Latvia's 2005 Criminal Procedures Law provides measures for the seizure and forfeiture of assets. The law enables law enforcement authorities to identify, trace, and confiscate criminal proceeds. Investigators can initiate an action for the seizure of assets recovered during a criminal investigation concurrently with the investigation itself—they do not need to wait until the investigation is complete. During the first 10 months of 2008, the courts returned 9 decisions, leading to the seizure of more than $7 million worth of assets on behalf of the state. Proceeds from asset seizures and forfeitures go into the state treasury.

The Prosecutor General's Office maintains a specialized staff to prosecute cases linked to money laundering. The seven staff prosecutors have undergone a special clearance process. In 2007, the Prosecutor General's Office received 27 money laundering cases for the prosecution of 53 individuals. The court examined twelve cases, and convicted 20 individuals, four of whom received sentences that included jail time. During the first 10 months of 2008 the Prosecutor's Office received 12 money laundering cases for the prosecution of 17 individuals, and 11 money laundering cases were examined by the court resulting in the sentencing of 18 people, five of whom were sentenced to prison.

The GOL has initiated measures aimed at combating the financing of terrorism. Article 88-1 of the Criminal Code criminalizes terrorist financing, and meets the United Nations Security Council Resolution (UNSCR) 1373 requirements. It has issued regulations to implement the sanctions imposed by UNSCR 1267. The regulations require that financial institutions report to the Control Service, transactions related to any individual or organization on the UNSCR 1267 Sanctions Committee's consolidated list or on other terrorist lists, including those shared with Latvia by international partners. The Control Service maintains consolidated terrorist finance and watch-lists and regularly distributes these to financial and nonfinancial institutions, as well as to their supervisory bodies. On several occasions, Latvian financial institutions have temporarily frozen monetary funds associated with names on terrorist finance watch lists, including those issued by the U.S. Office of Foreign Assets Control (OFAC), although authorities have found no confirmed matches to names on the list. Article 17 of the AML law authorizes the Control Service to freeze the accounts and funds of persons included on one of the terrorist lists for up to six months. The Control Service can also freeze accounts if it suspects terrorist financing. The AML law authorizes the Control Service to freeze the funds of persons designated on one of the terrorist lists for up to six months. If there is a case of possible terrorism financing, but the entity in question is not on one of the lists, the FIU can freeze funds for 45 days, which is the same interval as allowed for other crimes.

Latvia employs the same freezing mechanism with regard to terrorist assets as it uses with those relating to other crimes but includes involvement by the Latvian Security Police. Authorities handle associated investigations, asset and property seizures, in accordance with the Criminal Procedures Law.

In April 2005, the United States outlined concerns in a Notices of Proposed Rulemaking against two Latvian banks, under Section 311 of the USA PATRIOT Act. Both banks were found to lack adequate AML/CTF controls and were used by criminal elements to facilitate money laundering, particularly through shell companies. However, the FCMC pursued strong measures to clean up the banking

system. In August 2006, the United States rescinded the Proposed Notice of Rulemaking for one of the banks, but issued a final rule imposing a special measure against the second bank, VEF Banka, as a financial institution of primary money laundering concern. This measure, specific to VEF Banka, is still in effect.

Latvia permits only conventional money remitters (such as Western Union and Moneygram). The remitters work through some banks and not as separate entities. Alternative remittance services are prohibited in Latvia. The Control Service has not detected any cases of charitable or nonprofit entities used as conduits for terrorist financing in Latvia.

Latvia is a party to the UN Convention for the Suppression of the Financing of Terrorism and eleven other multilateral counterterrorism conventions. Latvia is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. A Mutual Legal Assistance Treaty (MLAT) has been in force between the United States and Latvia since 1999. Latvia is a member of MONEYVAL, a FATF-style regional body. In December 2007, MONEYVAL approved Latvia's progress report, which addressed shortcomings identified in the MER, and outlined Latvia's plan to attain full compliance with the FATF Recommendations.

Despite the legislative and regulatory improvements, Latvia still faces significant money laundering threats tied to corruption, organized crime and nonresident account holders. The GOL should enact additional amendments to its legislation to tighten its AML framework. It should continue to implement and make full use of the 2005 amendments to its Criminal Procedures Law and continue to actively implement and vigorously enforce the new AML law. It is also vital that competent authorities be provided adequate resources and staffing to carry out their duties under the new AML law. Latvia should continue to strengthen its risk-based approach to AML/CTF and take steps to further enhance the preventative aspects of its AML/CTF regime, including ensuring effective implementation of customer due diligence requirements and increased scrutiny of higher risk categories of transactions, clients and countries. The GOL should continue to take steps to increase information sharing and cooperation between law enforcement agencies at the working level. The GOL also should work toward increasing its authorities' ability and effectiveness in aggressively prosecuting and convicting those involved in financial crimes.

Lebanon

Lebanon is a financial hub for banking activities in the Middle East and eastern Mediterranean and has one of the more sophisticated banking sectors in the region. The banking sector continues to record an increase in deposits and as of late 2008, there were 66 banks (50 commercial banks, 12 investment banks, and four Islamic banks) operating in Lebanon with total deposits of $76 billion. Banque du Liban, the Central Bank of Lebanon (CBL), regulates all financial institutions and money exchange houses.

Lebanon faces significant money laundering and terrorist financing vulnerabilities. For example, Lebanon has a substantial influx of remittances from expatriate workers and family members, estimated by banking sources to reach $5 to $5.5 billion yearly. It has been reported that a number of these family ties are involved in underground finance and trade-based money laundering (TBML). Laundered criminal proceeds come primarily from domestic criminal activity and organized crime. In May 2007, for example, members of the terrorist group Fatah Al-Islam stole $150,000 from a BankMed branch in the northern city of Tripoli just before launching an attack against the Lebanese Armed Forces (LAF) surrounding the Nahr El-Bared refugee camp. There is some smuggling of cigarettes and pirated software, but the sale of these goods does not generate large amounts of funds that are then laundered through the formal banking system. There is a black market for stolen cars,

counterfeit goods and pirated software, CDs, and DVDs. The domestic illicit narcotics trade is not a principal source of money laundering proceeds.

In 2001, Lebanon enacted its anti-money laundering (AML) legislation, Law No. 318. This legislation created a framework for lifting bank secrecy, broadening the criminalization of money laundering beyond drugs, mandating suspicious transaction reporting, requiring financial institutions to obtain customer identification information, and facilitating access to banking information and records by judicial authorities. Under this law, money laundering is a criminal offense and punishable by imprisonment for a period of three to seven years and by a fine of no less than 20 million Lebanese pounds (approximately $13,315). The provisions of Law No. 318 expand the type of financial institutions subject to the provisions of the Banking Secrecy Law of 1956, to include institutions such as exchange offices, financial intermediation companies, leasing companies, mutual funds, insurance companies, companies promoting and selling real estate and construction, and dealers in high-value commodities. In addition, Law No. 318 requires companies engaged in transactions for high-value items (i.e., precious metals, antiquities, etc.) and real estate to report suspicious transactions. These companies are also required to ascertain the client's identity and address and retain records for a minimum of five years.

All financial institutions and money exchange houses are regulated by Law No. 318, which clarifies the Central Bank's powers to: require financial institutions to identify all clients, including transient clients; maintain records of customer identification information; request information about the beneficial owners of accounts; conduct internal audits; and, exercise due diligence in conducting transactions for clients. The Central Bank regulates private couriers who transport currency. Money service businesses, such as Western Union and Money Gram, must be licensed by the Central Bank and are subject to the provisions of this law. Charitable and nonprofit organizations must be registered with the Ministry of Interior and are required to have proper corporate governance, including audited financial statements. These organizations are also subject to the same suspicious activity reporting requirements.

Law No. 318 also established Lebanon's financial intelligence unit (FIU), the Special Investigation Commission (SIC). The SIC is an independent entity with judicial status that receives reports of suspicious transactions, investigates money laundering operations, monitors compliance of banks and other financial institutions, and issues financial advisories pursuant to the provisions of Law No. 318. The SIC serves as the key element of Lebanon's anti-money laundering/countering the finance of terrorism (AML/CTF) regime and is the only entity with the authority to lift bank secrecy for administrative and judicial agencies. It is also the administrative body through which foreign FIU requests for assistance are processed. The SIC joined the Egmont Group of FIUs in 2003.

Although offshore banking, trust and insurance companies are not permitted in Lebanon, the government enacted Law No. 19 on September 5, 2008, expanding existing provisions regarding activities of offshore companies and transactions committed outside Lebanon or in the Lebanese Customs Free Zone. All offshore companies must register with the Beirut Commercial Registrar, and the owners of an offshore company must submit a copy of their identification. Moreover, the Beirut Commercial Registrar maintains a special register, containing all relevant information about offshore companies.

There are two free trade zones (FTZ) operating in Lebanon: the Port of Beirut and the Port of Tripoli. FTZs fall under the supervision of the Customs Authority. Exporters moving goods into and out of the free zones submit a detailed manifest to Customs. Customs is required to inform the SIC on suspected TBML or terrorist financing, however, high-levels of corruption within Customs create vulnerabilities for TBML and other threats. Companies using the FTZ must be registered and must submit appropriate documentation, which is kept on file for a minimum of five years. Lebanon has no cross-border currency reporting requirements, presenting a significant cash-smuggling vulnerability.

However, since January 2003, Customs staff checks travelers randomly and notifies the SIC upon discovery of unspecified large amounts of cash.

In February 2004, Lebanon passed Law No. 645 requiring diamond traders to seek proper certification of origin for imported diamonds, and the Ministry of Economy and Trade (MOET) is in charge of issuing certification for re-exported diamonds. This law was designed to prevent the trafficking of "conflict diamonds" and allowed Lebanon to participate in the Kimberley Process in September 2005. Prior to this legislation, Lebanon had passed a decree in August 2003 prohibiting imports of rough diamonds from countries that are not participants in the Kimberley Process. Nonetheless, there have been consistent reports that some Lebanese diamond brokers in Africa are engaged in the laundering of diamonds—the most condensed form of physical wealth in the world. The Kimberley Process office in Lebanon notes, however, that according to the Kimberley Process procedure, diamond dealers must submit an application to MOET in order to import or export rough diamonds. The Beirut International Airport is the sole entry point for rough diamonds, and the Kimberley Process office at the Beirut International Airport monitors and physically checks the quantities of rough diamonds imported, ensuring that importers have a Kimberley Process certification issued by the country of origin. This office also checks on exports of rough diamonds from Lebanon to other member countries of the Kimberley Process. In 2007, Customs had two cases where they seized smuggled rough diamonds that did not have a Kimberley certification. Customs kept the rough diamonds in custody and notified the Kimberley Process office at MOET. The Kimberley Process Committee referred the two cases to the State Prosecutor, and both cases are now in the Lebanese court. As of late 2008, no additional cases of illegal diamond trade were reported. However, existing safeguards do not address the issue of smuggled diamonds, the purchase of fraudulently obtained Kimberley Process certificates, the laundering of diamonds, or value transfer via the diamond trade.

Lebanon has a large expatriate community throughout the Middle East, Africa, Australia, and parts of Latin America. They often work as brokers and traders, some of which network via family ties and are involved with underground finance and TBML. Informal remittances and value transfer in the form of trade goods add substantially to the remittance flows from expatriates via official banking channels. For example, some expatriate Lebanese brokers are actively involved in the trade of counterfeit goods in the tri-border region of South America, where the borders of Argentina, Brazil and Paraguay intersect, and the smuggling and laundering of diamonds in Africa. There are also reports that some in the Lebanese expatriate business community willingly or unwillingly give "charitable donations" to representatives of Hizballah, a U.S. designated foreign terrorist organization based in Lebanon.

Since its inception, the SIC has been active in providing support to international criminal case referrals. From January through October 2008, the SIC investigated 153 cases involving allegations of money laundering, terrorism, and terrorist financing activities. Out of the 153 cases, three of them were related to terrorist financing, and the SIC froze the accounts of eleven individuals totaling approximately $38,000. Additionally, bank secrecy regulations were lifted in 48 instances, and eight cases were transmitted by the SIC to the general state prosecutor for further investigation. As of October 2008, two cases were transmitted by the general state prosecutor to the penal judge. The general state prosecutor reported 15 cases to the SIC, three of which were related to embezzlement and counterfeiting charges, one to fraud, another to terrorism, two to drugs, and one to organized crime. However, as of late 2008 there has not been any money laundering convictions.

Throughout 2003, Lebanon adopted additional measures to strengthen efforts to combat money laundering and terrorist financing through a variety of ways, including the establishment of AML units in customs and the police. According to the SIC, inter-agency cooperation with other Lebanese law enforcement units, including customs, police, and the office of the general state prosecutor has increased. In 2005, a SIC Remote Access Communication system was created for the exchange of information between the SIC, customs, the Internal Security Forces (ISF) anti-money laundering and terrorist financing unit, and the general state prosecutor. By late 2008, continued cooperation led to the

transfer of over 75 suspicious transactions reports (STRs) to the SIC, allowing it to initiate several investigations based on the information.

In 2003, Lebanon also adopted Laws 547 and 553. Law 547 expanded Article One of Law No. 318, criminalizing any funds resulting from the financing or contribution to the financing of terrorism or terrorist acts or organizations based on the definition of terrorism as it appears in the Lebanese Penal Code. Such definition does not apply to Hizballah, which is considered a legitimate political party—represented by members of Parliament and a Cabinet minister—and resistance organization in Lebanon. The widespread view of Hizballah as a legitimate resistance organization, and thus not subject to Lebanese anti- terror financing laws, poses terrorist financing threats.

Law 547 also criminalized acts of theft or embezzlement of public or private funds, as well as the appropriation of such funds by fraudulent means, counterfeiting, or breach of trust by banks and financial institutions for such acts that fall within the scope of their activities. It also criminalized counterfeiting of money, credit cards, debit cards, and charge cards, or any official document or commercial paper, including checks. Law 553 expanded the definition of Article 316 of the Penal Code on terrorist financing, which stipulates that any person who voluntarily, either directly or indirectly, finances or contributes to terrorist organizations or terrorist acts is punishable by imprisonment with hard labor for a period not less than three years and not more than seven years, and a fine not less than the amount contributed but not exceeding three times that amount.

Lebanese law allows for property forfeiture in civil as well as criminal proceedings. The Government of Lebanon (GOL) enforces existing drug-related asset seizure and forfeiture laws, allowing for the confiscation of assets determined to be related to or proceeding from money laundering or terrorist financing. Both vehicles helped to transport illegal goods, such as drugs, as well as legitimate businesses established from illegal proceeds are also subject to seizure under Law 318. Forfeitures are then transferred to the Lebanese Treasury.

The SIC circulates the names of suspected terrorists individuals and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list, and the list of Specially Designated Global Terrorists designated by the U.S. pursuant to Executive Order 13224, and by the European Union under their relevant authorities to all financial institutions. As of early November 2008, the SIC signed nineteen memoranda of understanding with counterpart FIUs concerning international cooperation. Lebanon does not have a mutual legal assistance agreement with the United States.

In September 2007 the Lebanese Cabinet established a National Committee to suppress the financing of terrorism, chaired by the Ministry of Interior. The Cabinet expanded membership of The National Committee for coordinating AML policies to include representatives from the Ministries of Justice, Finance, Interior, Foreign Affairs, Economy, and a representative from the Beirut Stock Exchange. On October 8, 2008, the Parliament approved Law 32, which expanded the scope of investigators' field of inquiry, granting them greater authority to include funds originating from corruption activities into money laundering cases.

Lebanon is a member of the Middle East and North Africa Financial Action Task Force (MENAFATF) and is scheduled to undergo its first MENAFATF Mutual Evaluation. Lebanon is a party to the 1988 UN Drug Convention, and the UN Convention against Transnational Organized Crime. On October 8, 2008, the Parliament agreed that Lebanon would adhere to standards of the UN Convention against Corruption, although it is not currently a party to that instrument. Lebanon is not a party to the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Lebanon should encourage more efficient cooperation between financial investigators and other relevant agencies such as customs, police, and internal security forces. There should be more emphasis on linking predicate offenses to money laundering and not an over-reliance on suspicious transaction reports filed by financial institutions to initiate investigations. Lebanese law

enforcement authorities should examine domestic ties to the international network of Lebanese brokers and traders that are commonly found in underground finance, trade fraud, and TBML. Although the number of suspicious transaction reports filed and subsequent money laundering investigations coordinated by the SIC have steadily increased, prosecutions and convictions are still lacking. The end of the Syrian military occupation in April 2005 and the gradual decline of Syrian influence over the economy (both licit and illicit), security services, and political life in Lebanon may present an opportunity for the GOL to further strengthen its efforts against money laundering, corruption, and terrorist financing. The GOL should pass legislation to mandate and enforce cross-border currency reporting, upholding FATF Special Recommendation IX. Finally, the GOL should become a party to the UN International Convention for the Suppression of Terrorist Financing and to the UN Convention against Corruption.

Liechtenstein

The Principality of Liechtenstein has a well-developed offshore financial services sector, liberal incorporation and corporate governance rules, relatively low tax rates, and a tradition of strict bank secrecy. All of these conditions significantly contribute to the ability of financial intermediaries in Liechtenstein to attract funds from abroad. These same conditions have historically made the country attractive to money launderers. Although accusations of misuse of Liechtenstein's banking system persist, the Principality has made substantial progress in its efforts against money laundering in recent years.

Liechtenstein's financial services sector includes 15 banks, three nonbank financial companies, 16 public investment companies, and a number of insurance and reinsurance companies. The three largest banks control 90 percent of the market. Liechtenstein's 389 licensed fiduciary companies and 60 lawyers serve as nominees for or manage more than 75,000 entities (mostly corporations or trusts) available primarily to nonresidents of Liechtenstein. Approximately one third of these entities hold controlling interests in separate entities chartered outside of Liechtenstein. Laws permit corporations to issue bearer shares.

Liechtenstein's anti-money laundering/counterterrorist financing (AML/CTF) regime was evaluated in 2007 by the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), a Financial Action Task Force (FATF)-style regional body. The evaluation notes that fiscal offenses, including serious and organized fiscal fraud, are not predicate offenses for money laundering in Liechtenstein. The report also recommends Liechtenstein provide for criminal liability for corporate entities. Additional, as yet uncorrected, items are noted throughout this report. Liechtenstein remains on an Organization for Economic Cooperation and Development (OECD) list of "noncooperative" countries in terms of provision of tax information.

Narcotics-related money laundering has been a criminal offense in Liechtenstein since 1993. Under Article 165 of the Criminal Code, money laundering is punishable by imprisonment of up to five years or a fine of up to 360,000 Swiss francs (approximately $322,250). Under Article 278a, a member of a criminal organization is subject to a punishment of up to ten years imprisonment. In principle, violations of the Due Diligence Act are punished with imprisonment of up to six months or a fine of up to 360,000 Swiss francs (approximately $322,250). The Office of the Prosecutor and the Court of Justice are responsible for investigating these offenses. The National Police also maintains a special unit for combating economic crimes.

Liechtenstein enacted its first general anti-money laundering (AML) legislation in 1996. Although this law applies some money laundering controls to financial institutions and intermediaries operating in Liechtenstein, the AML regime at that time suffered from serious systemic problems and deficiencies.

In response to international pressure, the Government of Liechtenstein (GOL) took legislative and administrative steps to improve its AML regime.

Since 2000, far-reaching legislative reforms have been undertaken in the course of strengthening and modernizing the financial center, such as the creation of the financial intelligence unit (FIU) in 2001 and the Financial Market Authority (FMA) in 2005. Other key reforms include the total revision of and subsequent amendments to the Mutual Legal Assistance Act (2000 and 2006); several amendments to the Insurance Supervision Act (2002 and 2005); the counterterrorism package (2003); the total revision of the Due Diligence Act (2004) and the Investment Undertakings Act (2005); the creation of an Asset Management Act (2005) and a Market Abuse Act (2006); several amendments to the Narcotics Act (2006); key changes to the Banking Act (2006 and 2007); and the total revision of the Securities Prospectus Act (2007) and the Pension Funds Act.

Liechtenstein's primary piece of AML legislation, the Due Diligence Act (DDA), applies to banks, e-money institutions, casinos, dealers in high-value goods, and a number of other entities. Along with the Due Diligence Ordinance, the DDA sets out the basic requirements of the AML regime in accordance with the FATF Forty-Nine Recommendations in the areas of customer identification, suspicious transaction reporting, and record keeping. Liechtenstein has established an overall risk-based approach that requires financial institutions to build and keep up to date a profile for each long-term customer. The DDA prohibits banks and postal institutions from engaging in business relationships with shell banks and from maintaining bearer-payable passbooks, accounts, and deposits.

The suspicious transaction reporting requirement applies to banks, insurers, financial advisers, postal services, exchange offices, attorneys, financial regulators, casinos, and other entities. The GOL has reformed its suspicious transaction reporting system to permit reporting for a much broader range of offenses than in the past. The reporting requirement now uses the basis of a "suspicion," rather than the previous standard of "a strong suspicion." However, the 2007 MONEYVAL mutual evaluation identifies Liechtenstein's rules on "tipping off" the subject of a suspicious transaction report (STR) as inadequate. Filers of STRs are prohibited from "tipping off" only for a period of 20 days. The report also recommends the STR requirement encompass attempted occasional transactions.

On June 23, 2008, the GOL announced it would implement legislation requiring that money transfers above 25,000 Swiss francs (approximately $17,900) include information on the identity of the sender, including his or her name, address, and account number. The proposed measures will ensure that this information will be immediately available to appropriate law enforcement authorities. The information will assist them in detecting, investigating, and prosecuting money launderers, terrorist financiers, and other criminals.

The FMA serves as Liechtenstein's central financial supervisory authority. FMA has assumed the responsibilities of several former administrative bodies, including the Financial Supervisory Authority and the Due Diligence Unit, both of which once exercised responsibility over money laundering issues. FMA reports exclusively to the Liechtenstein Parliament, making it independent from Liechtenstein's government. The FMA supervises a large variety of financial actors, including banks, finance companies, insurance companies, currency exchange offices, and real estate brokers. FMA works closely with Liechtenstein's FIU, the Office of the Prosecutor, and the police.

Liechtenstein's FIU, the Einheit fuer Finanzinformationen (EFFI), receives, analyzes and disseminates STRs relating to money laundering and terrorist financing. The EFFI has access to various governmental databases. However, EFFI cannot seek additional financial information unrelated to filed STRs. In 2007, the EFFI received 207 STRs, a 27 percent increase compared to the 163 STRs in 2006. Banks submitted 130 STRs, professional trustees submitted 64, lawyers six, investment companies three, and the Postal Service one. Three STRs were submitted by Liechtenstein authorities and the FMA. Three percent of the subjects of STRs were U.S. nationals. In 2007, the FIU received

140 inquiries from 24 FIUs and sent 127 inquiries to 24 FIUs. Information regarding the number of STRs received in 2008 is not yet available.

STRs have generated several successful money laundering investigations. EFFI works closely with the prosecutor's office and law enforcement authorities, in particular with a special economic and organized crime unit of the National Police known as EWOK. However, the 2007 MONEYVAL evaluation of Liechtenstein notes the number of investigations triggered by the FIU is low. The report also notes Liechtenstein's tendency to transfer cases to the authorities of the jurisdiction where the offense occurred keeps the judiciary from developing its own experience and jurisprudence in money laundering matters. There have been only two prosecutions in Liechtenstein for autonomous money laundering and no convictions.

Liechtenstein has legislation to seize, freeze, and share forfeited assets with cooperating countries. The special Law on Mutual Assistance in International Criminal Matters gives priority to international agreements. Money laundering is an extraditable offense, and Liechtenstein grants legal assistance on the basis of dual criminality. Article 253a of the Code of Criminal Procedure provides for the sharing of confiscated assets. Liechtenstein has not adopted the policy of reversing the burden of proof (i.e., forcing a defendant to prove assets were legally obtained instead of the state being required to prove their illicit nature.)

A series of amendments to Liechtenstein laws, along with amendments to the Criminal Code and the Code of Criminal Procedure, criminalize terrorist financing. Liechtenstein has implemented UNSCRs 1267 and 1333. The GOL can freeze the accounts of individuals and entities that are designated pursuant to these UNSCRs, and as of 2007, had blocked approximately $150,000 worth of terrorist assets under the 1267 regime. The GOL has not, however, established a national terrorist list, and therefore lacks measures to freeze and manage assets suspected of belonging to suspected terrorists that are not on a UN list. The GOL updates its implementing ordinances regularly.

The GOL is reviewing the Criminal Code to further expand the list of predicate offenses, including terrorist financing activities. The revision is expected to implement the following articles to the Criminal Code: draft Article 278b will allow punishment of leaders of a terrorist group with five to fifteen years imprisonment, and members or financial supporters of a terrorist group with imprisonment of one to ten years; draft Article 278c will list terrorist offenses; and draft Article 278d will address terrorist financing. There have been no terrorist financing cases yet.

The GOL has improved its international cooperation provisions in both administrative and judicial matters. A mutual legal assistance treaty (MLAT) between Liechtenstein and the United States entered into force on August 1, 2003. The U.S. Department of Justice has acknowledged Liechtenstein's cooperation in the Al-Taqwa Bank case and in other fraud and narcotics cases. The FIU has in place memoranda of understanding with nine FIUs, and seven others are under negotiation.

Liechtenstein is a member of MONEYVAL, and EFFI is a member of the Egmont Group. The GOL is a party to the UN Convention for the Suppression of the Financing of Terrorism. On March 9, 2007, Liechtenstein acceded to the 1988 UN Drug Convention, and on February 20, 2008, it ratified the UN Convention against Transnational Organized Crime. Liechtenstein is not a party to the UN Convention against Corruption.

While the Government of Liechtenstein has made progress in addressing the shortcomings in its AML regime, it should continue to build upon the foundation of its evolving AML/CTF regime. The GOL should prohibit the issuance and use of corporate bearer shares and establish the criminal liability of corporate entities. Liechtenstein also should expand its list of predicate offenses to ensure all appropriate crimes are addressed, as well as prohibit " tipping of"—a practice that permits account holders to transfer funds in question and mitigates thorough investigation by law enforcement and the possibility of criminal prosecution. The FIU should have access to additional financial information

related to STRs. Liechtenstein also should consider creating a national terrorist list, which would allow for the implementation of UNSCRs that do not include a list, such as UNSCR 1373. While Liechtenstein recognizes the rights of third parties and protects uninvolved parties in matters of confiscation, the government should distinguish between bona fide third parties and others. Liechtenstein should ratify the UN Convention against Corruption.

Luxembourg

Despite its standing as the second-smallest member of the European Union (EU), Luxembourg is one of the largest financial centers in the world. While Luxembourg is not a major hub for illicit narcotics distribution, the size and sophistication of its financial sector create opportunities for money laundering, tax evasion, and other financial crimes. Luxembourg is an offshore financial center. Although there are a handful of domestic banks operating in the country, the majority of banks registered in Luxembourg are foreign subsidiaries of banks in Germany, Belgium, France, Italy, and Switzerland. A significant share of Luxembourg's suspicious transaction reports (STRs) are generated from transactions involving clients in these countries. Luxembourg's strict bank secrecy laws allow international financial institutions to benefit from and operate a wide range of services and activities. With over $2,400,000,000,000 in domiciled assets, Luxembourg is the second largest mutual fund investment center in the world, after the United States. As of October 2008, 154 registered banks existed, with a collective balance sheet total reaching approximately $1,300,000,000,000. In addition, as of September 2008, a total of 3,322 "undertakings for collective investment" (UCIs), or mutual fund companies, whose net assets had reached over approximately $2,400,000,000,000 operated from Luxembourg or traded on the Luxembourg stock exchange. Luxembourg has approximately 15,000 holding companies, 95 insurance companies, and 260 reinsurance companies. According to the latest figures available (2006) the Luxembourg Stock Exchange listed over 39,000 securities issued by nearly 4,100 entities from 105 countries. Luxembourg also has 116 registered venture capital funds (Société d'investissement en capital à risqué, or "SICAR").

The Government of Luxembourg (GOL) has enacted laws and adopted practices that help prevent the abuse of its bank secrecy laws and has implemented a comprehensive legal and supervisory AML regime. The Law of July 7, 1989, updated in 1998 and 2004, serves as Luxembourg's primary anti-money laundering (AML) and counterterrorist financing (CTF) law, criminalizing the laundering of proceeds for an extensive list of predicate offenses, including narcotics-trafficking. The laws provide customer identification, recordkeeping, and STR requirements. Corruption, weapons offenses, fraud committed against the EU and organized crime are on Luxembourg's list of predicate offenses for money laundering. The entities subject to money laundering regulations include banks, pension funds, insurance brokers, UCIs, management companies, external auditors, accountants, notaries, lawyers, casinos, gaming establishments, real estate agents, tax and economic advisors, domiciliary agents, insurance providers, and dealers in high-value goods such as jewelry and vehicles. All obliged entities are required to file STRs with the financial intelligence unit (FIU). The law also imposes strict "know your customer" (KYC) requirements on obliged entities for all customers, including beneficial owners, trading in goods worth at least 15,000 euros (approximately $20,250). If the transaction or business relationship is remotely based, the law details measures required for customer identification. Entities must proactively monitor their customers for potential risk. Luxembourg's laws also prohibit "tipping off." Financial institutions must ensure adequate internal organization and employee training, and must cooperate with authorities.

A new law, issued on July 17, 2008, contains further provisions on customer due diligence and other internal risk management measures to prevent money laundering and terrorist financing. This legislation also requires that proper, accurate, and current information be available about the contracting party to ensure transparency. This law widens the scope of predicate offenses and sets

forth minimum sentencing guidelines for money laundering offenses to comport with the Financial Action Task Force (FATF) recommendations.

Although Luxembourg is well known for its strict banking secrecy laws, these laws do not apply in investigations and prosecutions of money laundering and other crimes. A court order is not necessary for the competent authorities to investigate account information in suspected money laundering cases or in response to an STR. Financial professionals have a legal obligation to cooperate with the public prosecutor in investigating such cases. To obtain a conviction for money laundering, prosecutors must prove criminal intent rather than negligence. Negligence, however, is subject to scrutiny by a competent authority, with sanctions for noncompliance varying from 1,250 to 1,250,000 euros (approximately $1,700 to $1,687,500) to, potentially, forfeiture of the professional license. Luxembourg's regulatory authorities believe these fines to be stiff enough so as to encourage strict compliance.

The Financial Supervision Commission, Commission de Surveillance du Secteur Financier (CSSF), is an independent body under the Ministry of Finance that acts as the supervisory authority for banks, credit institutions, the securities market, some pension funds, financial sector professionals, and other financial sector entities covered by the country's AML/CTF laws. Banks must undergo audits under CSSF supervision. All entities involved in oversight functions, including registered independent auditors, in-house bank auditors, and the CSSF, can obtain the identities of the beneficial owners of accounts. The CSSF establishes the standards for and grants "financial sector professional" (PSF) status to financial sector entities. Originally covering only individual financial sector professionals having access to customer information subject to bank secrecy laws, the CSSF recently established a sub-category for service providers with potential access to that information, such as transaction-clearing houses, information technology consultants, and data warehousing services. With this status, banks have the flexibility to outsource some services while guaranteeing continued compliance with banking secrecy laws to their customers. The CSSF regulates the PSF status tightly, frequently issuing circulars and updating accreditation requirements. As of October 31, 2008, a total of 260 PSFs operate in Luxembourg.

The Luxembourg Central Bank oversees the payment and securities settlement system, and the Insurance Commissioner's Office, Commissariat aux Assurances, (CAA), under the Ministry of Finance, is the regulatory authority for the insurance sector.

SICAR entities are covered by a law adopted in July 2007. Adopted at the same time was a law regulating markets dealing in financial instruments. Two grand-ducal regulations augment the law. The first outlines organizational requirements and rules of conduct in the financial sector; and the second establishes the need to keep an official listing for financial instruments.

Under the direction of the Ministry of the Treasury, the CSSF has established the Anti-Money Laundering Steering Committee, Comité de Pilotage Anti-Blanchiment (COPILAB), composed of supervisory and law enforcement authorities, the FIU, and financial industry representatives. The committee meets monthly to develop a common public-private approach to strengthen Luxembourg's AML regime.

Luxembourg's laws and regulations do not distinguish between onshore and offshore activities. Foreign institutions seeking establishment in Luxembourg must demonstrate prior establishment in a foreign country and meet stringent minimum capital requirements. Companies must maintain a registered office in Luxembourg. Authorities perform background checks on all applicants and a government registry publicly lists company directors. Nominee (anonymous) directors are not permitted.

Luxembourg permits bearer shares. Officials contend that bearer shares do not pose a money laundering concern because KYC laws require banks to know the identities of beneficial owners.

Luxembourg's FIU, Cellule de Renseignement Financier, is part of the State Prosecutor's Office and housed within Luxembourg's Ministry of Justice. The FIU consists of four State Prosecutors and one analyst. The FIU State Prosecutors pursue economic and financial crimes in Luxembourg and spend significant portions of their time preparing for cases involving financial crimes. They are also occasionally called upon to prosecute cases not involving financial crimes.

The FIU receives and analyzes the STRs from all obliged entities. The FIU provides members of the financial community with access to updated information on money laundering and terrorist financing practices. The FIU issues circulars to all financial sector-related professionals who are not regulated under the CSSF as well as notifies the financial sector about terrorist financing designations promulgated by the EU and United Nations (UN).

By late November 2008, obliged institutions filed a total of 901 STRs, compared to a total of 811 in 2007. This increase of STRs is mainly due to the establishment of PayPal in Luxembourg in July 2007. So far in 2008, 238 STRs have been submitted by PayPal. The banking sector submits the largest volume of STRs. STRs submitted by the fund investment sector remain rare despite the general economic evolution of that sector. In 2007, 225 information requests were received from foreign authorities, compared to 180 in 2006. Since 85 percent of the subjects of STRs reside abroad, the efficiency of Luxembourg's AML system heavily depends on the international cooperation between FIUs and between judicial authorities. The 2008 statistics on the number of U.S. residents referenced in STRs are not available yet. Among the individuals referenced in STRs in 2007, 67 resided in the U.S. Of the 343 cases of suspicious activity in 2007, 32 percent related to organized crime (including terrorist financing) and eight percent involved suspected narcotics-related money laundering.

The GOL prosecuted three money laundering cases in 2006 and four in 2007. In May 2006, two individuals were convicted of laundering narcotics-trafficking proceeds and received sentences of 72 months and 12 months of imprisonment. In November 2006, five individuals were acquitted of money laundering charges when the court found that the State had not sufficiently established the linkage between the funds and either narcotics-trafficking or an organized crime enterprise. The government closed this legal vulnerability with Bill 5756, which expands the list of predicate offenses. Also in November 2006, a Dutch lawyer representing a convicted drug trafficker was acquitted of attempted money laundering charges, but an appellate court overturned the acquittal in May 2007. The defendant appealed his conviction to Luxembourg's Supreme Court, which handed down a suspended sentence of four years and a 10,000 euro (approximately $13,500) fine. The money was confiscated by the Luxembourg authorities.

Luxembourg law only allows for criminal forfeitures and public takings. Narcotics-related proceeds are pooled in a special fund to invest in anti-drug abuse programs. Luxembourg can confiscate funds found to be the result of money laundering even if they are not the proceeds of a crime. The GOL can, on a case-by-case basis, freeze and seize assets, including assets belonging to legitimate businesses used for money laundering. The FIU freezes assets and issues blocking orders when necessary. The government has adequate police powers and resources to trace, seize, and freeze assets without undue delay. The banking community generally cooperates with enforcement efforts to trace funds and seize or freeze bank accounts. Luxembourg has independently frozen several accounts. This has resulted in court challenges by the account holders, after which nearly all of the assets were subsequently released. The GOL has a comprehensive system not only for the seizure and forfeiture of criminal assets, but also for the sharing of those assets with other governments. Bill 5019, of August 2007, allows Luxembourg to seize assets on the basis of a foreign criminal conviction, even when there is no specific treaty in place with that country.

The Ministry of Justice studies and reports on potential abuses of charitable and nonprofit entities. Justice and Home Affairs ministers from Luxembourg agreed in early December 2005, to take into account five principles with regard to nonprofit organizations: safeguarding the integrity of the sector;

dialogue with stakeholders; continuing knowledge development of the sector; transparency, accountability and good governance; and effective, proportional oversight.

Luxembourg's authorities have not found evidence of the widespread use of alternative remittance systems or trade-based money laundering. Government officials maintain that because AML rules would apply to such systems, they are not considering separate legislative or regulatory initiatives to address them.

The GOL actively disseminates to its financial institutions information concerning suspected individuals and entities on the UNSCR 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to Executive Order 13224. Luxembourg's authorities can and do take action against groups targeted through both the UN and EU designation processes. Luxembourg does not have legal authority to independently designate terrorist groups or individuals. The government has been working on legislation with regard to this issue for more than three years, but the legislation remains in the drafting process. Government prosecutors are confident they could use existing judicial authority if any institution were to identify a terrorist financier. Although bilateral freeze requests have a limit of three months, designations under the EU, UN, or international investigation processes continue to be subject to freezes for an indefinite time period.

Luxembourg cooperates with, and provides assistance to foreign governments in their efforts to trace, freeze, seize and forfeit assets. During 2007, Luxembourg responded to four Mutual Legal Assistance Treaty (MLAT) requests from the U.S. Government (USG) and in return requested USG assistance in three cases. Dialogue and other bilateral proceedings between Luxembourg and the United States have been extensive. Upon request from the USG, Luxembourg froze the bank accounts of individuals suspected of involvement in terrorism. Luxembourg also worked closely with the U.S. Department of Justice throughout 2007 on several drug-related money laundering cases as well as one possible terrorist financing case. In October 2006, the USG and the GOL announced a sharing agreement in which they would divide equally 11,366,265 euros (then approximately $14,548,820) of forfeited assets of two convicted American narcotics-traffickers who had deposited the monies in Luxembourg bank accounts. Luxembourg has placed a priority on progressing with the legal instruments implementing the extradition and mutual legal assistance agreements the USG signed with the EU in 2003. In December 2007, the Luxembourg Parliament gave final approval to both the bilateral U.S.-Luxembourg and multilateral U.S.-EU extradition and mutual legal assistance agreements.

Luxembourg is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. On May 12, 2008, Luxembourg ratified the UN Convention against Transnational Organized Crime.

Luxembourg is a member of the FATF, and the Luxembourg FIU is a member of the Egmont Group. Luxembourg and the United States have had a MLAT since February 2001. Luxembourg has consistently provided training and assistance in money laundering matters to officials in countries whose regimes are in the development stage.

However, the scarce number of financial crime cases is of concern, particularly for a country that has such a large financial sector. The GOL should take action to delineate in legislation regulatory, financial intelligence, and prosecutorial activities among governmental entities in the fight against money laundering and terrorist financing. The situation is most acute regarding the lack of a distinct legal framework for the FIU whose staff, activities, and authorities are divided among at least four different ministries. The State Prosecutors in the FIU should be exempt from nonfinancial crime duties, and the FIU should increase the number of analytical staff to effectively analyze and disseminate the volume of STRs the FIU receives. The GOL should pass legislation creating the authority for it to independently designate those who finance terrorism as it would be well served to have such authority. The GOL also should enact legislation to address the continued use of bearer

shares. The GOL should continue its efforts to assist jurisdictions with nascent or immature AML/CTF regimes.

Macau

Under the one country/two systems principle that underlies Macau's 1999 reversion to the People's Republic of China, Macau has substantial autonomy in all areas of governance except defense and foreign affairs. Macau's free port, a lack of foreign exchange controls, and a rapidly expanding economy based on gambling and tourism create an environment that can be exploited for money laundering purposes. Macau's limited institutional capacity is a particular concern. The Macau Special Administrative Region (MSAR) is a gateway to China, and can be used as a transit point to remit funds and criminal proceeds to and from China. Further, Macau's economy is heavily dependent on gaming. The gaming sector continues to be a significant vulnerability. However, Macau is not a significant offshore financial center.

The primary money laundering methods in Macau's financial system are: wire transfers, currency exchange/cash conversion, bulk movement of cash, the use of casinos to remit or launder money, and the use of nominees, trusts, family members, or third parties to transfer cash. Crimes that occur in Macau include financial fraud, bribery, embezzlement, organized crime, counterfeiting, and drug-related crimes. However, there have been no reported instances of terrorism-related financial crimes. Crimes related to financial fraud appear to be increasing, while drug-related crimes are becoming less common.

The gaming sector and related tourism are critical parts of Macau's economy. Taxes from gaming in the first eleven months of 2008 increased by 38 percent from the same period in 2007 and comprised 77 percent of government revenue in the first eleven months of 2008. Gaming revenue in the first nine months of 2008 exceeded the 2007 total and account for well over 60 percent of Macau's GDP. The MSAR ended a long-standing gaming monopoly early in 2002 when it awarded concessions to two additional operators, the U.S.-based Las Vegas Sands and Wynn Corporations. Macau now effectively has six separate casino licensees operating 31 casinos, the three concession holders: Sociedade de Jogos de Macau (SJM), Galaxy and Wynn, and three sub-concession holders: Las Vegas Sands, MGM and PBL/Melco.

Under the old monopoly framework, organized crime groups were closely associated with the gaming industry through their control of VIP gaming rooms and activities such as racketeering, loan sharking, and prostitution. The VIP rooms are catered to clients seeking anonymity within Macau's gambling establishments, and received minimal official scrutiny. As a result, the gaming industry provided an avenue for the laundering of illicit funds and served as a conduit for the unmonitored transfer of funds out of China. VIP rooms continue to operate in Macau and are the primary revenue generators for Macau's casinos. Although the arrival of international gaming companies has improved management and governance in all aspects of casino operations, concerns about organized crime groups and poorly regulated junket operators' associations with VIP rooms remain. The MSAR's money laundering legislation aims to make money laundering by casinos more difficult by improving oversight, and tightening reporting requirements. On June 7, 2004, Macau's Legislative Assembly passed legislation allowing casinos and junket operators to make loans, in chips to customers, in an effort to prevent loan-sharking. The law requires both casinos and junket operators to register with the government.

Macau has taken steps over the past four years to improve its regulatory structure and institutional capacity to tackle money laundering. On March 23, 2006, the Macau Special Administrative Region Government (MSARG) passed a 12-article bill on the prevention and repression of money laundering that incorporates aspects of the revised FATF Forty Recommendations. The law expands the number of sectors covered by Macau's previous anti-money laundering (AML) legislation, includes provisions on due diligence, and broadens the definition of money laundering to include all serious predicate

crimes. The AML law also authorizes the interim establishment of a financial intelligence unit (FIU) for a term of three years, which began operation in November 2006. The law provides for 2-8 years imprisonment for money laundering offenses and if a criminal is involved in organized crime or triad-related money laundering, increases the penalties by one-half. The new law also allows for fines to be added to the time served and eliminates a provision reducing time served for good behavior.

The 2006 law also extends the obligation of suspicious transaction reporting to lawyers, notaries, accountants, auditors, tax consultants, and offshore companies. Covered businesses and individuals must meet various obligations, such as the duty to confirm the identity of their clients and the nature of their transactions. Businesses must reject clients that refuse to reveal their identities or type of business dealings. The law obliges covered entities, including casinos, to send suspicious transaction reports (STRs) to the relevant authorities and cooperate in any follow-up investigations.

Macau's financial system is governed by the 1993 Financial System Act and amendments, which lay out regulations to prevent use of the banking system for money laundering. The Act imposes requirements for the mandatory identification and registration of financial institution shareholders, customer identification, and external audits that include reviews of compliance with anti-money laundering statutes. The 1997 Law on Organized Crime criminalizes money laundering for the proceeds of all domestic and foreign criminal activities, and contains provisions for the freezing of suspect assets and instrumentalities of crime. Legal entities may be civilly liable for money laundering offenses, and their employees may be criminally liable.

The 1998 Ordinance on Money Laundering sets forth requirements for reporting suspicious transactions to the Judiciary Police and other appropriate supervisory authorities. These reporting requirements apply to all legal entities supervised by the regulatory agencies of the MSARG, including pawnbrokers, antique dealers, art dealers, jewelers, and real estate agents. In October 2002, the Judiciary Police set up the Fraud Investigation Section to receive STRs in Macau and to undertake subsequent investigations. In 2006, the newly established FIU assumed responsibility for receiving STRs and forwarding actionable reports to the Judiciary Police for investigation. In November 2003, the Monetary Authority of Macau issued a circular to banks, requiring that STRs be accompanied by a table specifying the transaction types and money laundering methods, in line with the collection categories identified by the Asia/Pacific Group on Money Laundering. Macau law provides for forfeiture of cash and assets that assist in or are intended for the commission of a crime. There is no significant difference between the regulation and supervision of onshore and of offshore financial activities.

The Macau criminal code (Decree Law 58/95/M of November 14, 1995, Articles 22, 26, 27, and 286) criminalizes terrorist financing. Macau does not have any provision or procedures for freezing terrorist related funds or assets outside normal judicial proceedings to fully implement UNSCRs 1267 and 1373. Although no special mechanism exists and a judicial order is required, the general framework of seizure and forfeiture of funds and assets under the Criminal Code and Criminal Procedure Code do provide the MSARG the authority to freeze terrorist assets. Macau financial authorities direct the institutions they supervise to conduct searches for terrorist assets, using the consolidated list provided by the UN 1267 Sanctions Committee and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. No terrorist assets were identified in 2008.

The Macau legislature passed a counterterrorism law in April 2002 to facilitate Macau's compliance with UNSCR 1373. The legislation criminalizes violations of UN Security Council resolutions, including counterterrorism resolutions, and strengthens counterterrorist financing provisions. When China ratified the UN International Convention for the Suppression of the Financing of Terrorism, China stipulated that the Convention would apply to the MSAR. On March 30, 2006, the MSARG passed additional counterterrorism legislation aimed at strengthening measures to counterterrorist financing (CTF). The law partially implements UNSCR 1373 by making it illegal to conceal or handle

finances on behalf of terrorist organizations. Individuals are liable even if they are not members of designated terrorist organizations themselves. The legislation also allows prosecution of persons who commit terrorist acts outside of Macau in certain cases, and would mandate stiff penalties. However, the legislation does not authorize the freezing of terrorist assets outside normal legal channels, nor does it discuss international cooperation on terrorist financing. In January 2005, the Monetary Authority of Macau issued a circular to all banks and other authorized institutions requiring them to maintain a database of suspected terrorists and terrorist organizations.

A Macau Monetary Authority official serves as the head of the FIU. The FIU has been expanding since its inception and now consists of more than ten staff, including members seconded from the Insurance Bureau, Monetary Authority and Judicial police. The FIU will continue to hire additional staff in 2009. The FIU works with the Macau Judicial Police on investigation of STRs and with the Public Prosecutors Office on prosecution of offenders. The FIU moved into permanent office space in January 2007 and is accepting STRs from banks, financial institutions and the Gaming Inspectorate. The three-year authorization for the FIU expires in 2009. FIU officials have assured the U.S. government that the organization will not be disbanded at the end of the current authorization. The government says it is planning to submit legislation institutionalizing the FIU in 2009. Alternatively, the organization could be authorized for an additional three years.

Increased attention to financial crimes in Macau since the events of September 11, 2001, has led to a general increase in the number of STRs; however, the number of STRs remains relatively low when compared others in the region. Macau's Judiciary Police received 109 STRs in 2004, 194 in 2005, 396 STRs from January to September 2006, and 557 STRs from January to September 2007. Figures for 2008 were unavailable. In 2004 Macau opened ten money laundering cases but prosecuted none. In 2005, Macau opened nine money laundering cases and prosecuted two. Since the entry into force of the new AML law in April 2006 through 2007, the Macau Public Prosecutions office received 23 suspected cases of money laundering from the FIU. Of these, 14 were referred for investigation by the Judicial Police or the Commission Against Corruption. Figures for 2008 were unavailable. Between 2005 and 2007, the Judicial Police referred three money laundering cases to the Public Prosecutions office. The MSARG has not shared information on the disposition of these cases.

In May 2002, the Macau Monetary Authority revised its anti-money laundering regulations for banks to bring them into greater conformity with international practices. Guidance also was issued for banks, moneychangers, and remittance agents, addressing record keeping and suspicious transaction reporting for cash transactions over U.S. $2,500. For such transactions, banks, insurance companies, and moneychangers must perform customer due diligence. However for casinos, Macau requires customer due diligence only for transactions above $62,500. In 2003, the Monetary Authority of Macau (AMCM) examined all moneychangers and remittance companies to determine their compliance with these regulations. The AMCM, in coordination with the IMF, updated its bank inspection manuals to strengthen anti-money laundering provisions. The AMCM inspects banks every two years, including their adherence to anti-money laundering regulations.

Former Secretary for Public Works and Transportation, Ao Man Long, was arrested December 2006 and charged with taking bribes and engaging in irregular financial activities, including corruption, money laundering, and abuse of power. The Macau Commission Against Corruption (CAC) reported that Ao had received bribes from real estate and construction companies in excess of $23 million in return for contracts and approvals in 20 public works projects. Ao, assisted by family members and others, used shell companies in Hong Kong and the British Virgin Islands to launder money. On January 30, 2008, Ao was convicted on 40 counts of bribe taking, 13 counts of money laundering, one count of holding assets from unknown sources and one count of incorrect declaration of assets. He was sentenced to 27 years in prison and U.S. $31.5 million of his assets were seized, including assets not directly linked to his corruption and money laundering cases. Ao's wife, Chan Meng-leng was sentenced in absentia to 23 years in jail. His father (Ao Vong-kong), younger brother (Ao Man-fu) and

sister-in-law (Chan Wa-choi) were convicted of 6-14 counts of money laundering, and were sentenced to 10-18 years. Three Macau businessmen were also convicted of bribery in connection with the case. The businessmen and Ao's family have appealed their convictions, Ao Man Long has not. The cooperation of the Hong Kong authorities was instrumental in the investigation of the case.

There is no requirement to report large sums of cash carried into Macau. The Macau Customs Service has the authority to conduct physical searches and detain suspicious persons and executes random checks on cross-border movement of cash, including record keeping when the amount of cash carried over the border exceeds U.S. $38,500. However, there is no central database for such reports. Mainland China does restrict the transport of RMB out of China. Persons may carry no more than Renminbi (RMB) 20,000 (approximately $2,750) per day out of China. According to the Macau Prosecutors Office, this Chinese requirement limits the number of people carrying large amounts of cash into Macau.

The United States has no formal law enforcement cooperation agreements with Macau, though informal cooperation between the United States and Macau routinely takes place. The Judiciary Police have been cooperating with law enforcement authorities in other jurisdictions through the Macau branch of Interpol, to suppress cross-border money laundering. In addition to Interpol, the Fraud Investigation Section of the Judiciary Police has established direct communication and information sharing with authorities in Hong Kong and Mainland China. In July 2006, the MSAR enacted the Law on Judicial Cooperation in Criminal Matters, enabling the MSAR to enter into more formal judicial and law enforcement cooperation relationships with other countries. The law became effective in November 2006. Macau's FIU has not yet established MOUs on information sharing with other jurisdictions but is currently negotiating with FIUs from Hong Kong, mainland China, Portugal, Japan, Korea, and Sri Lanka.

The Monetary Authority of Macau cooperates with other financial authorities. It has signed memoranda of understanding with the People's Bank of China, China's Central Bank, the China Insurance Regulatory Commission, the China Banking Regulatory Commission, the Hong Kong Monetary Authority, the Hong Kong Securities and Futures Commission, the Insurance Authority of Hong Kong, and Portuguese bodies including the Bank of Portugal, the Banco de Cabo Verde and the Instituto de Seguros de Portugal.

Macau participates in a number of regional and international organizations. It is a member of the Asia/Pacific Group on Money Laundering (APG), the Offshore Group of Banking Supervisors, the International Association of Insurance Supervisors, the Offshore Group of Insurance Supervisors, the Asian Association of Insurance Commissioners, the International Association of Insurance Fraud Agencies, and the South East Asia, New Zealand and Australia Forum of Banking Supervisors (SEAZA). In 2003, Macau hosted the annual meeting of the APG, which adopted the revised FATF Forty Recommendations and a strategic plan for anti-money laundering efforts in the region from 2003 to 2006. In ratifying the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption China in each case specified that the treaty would apply to the MSAR. Macau officials have taken a number of steps in the past three years to raise industry awareness of money laundering. The Macau Monetary Authority trains banks on anti-money laundering measures on a regular basis.

On September 15, 2005, the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN) designated Macau-based Banco Delta Asia (BDA) as a primary money laundering concern under Section 311 of the USA PATRIOT Act and issued a proposed rule regarding the bank, In its designation of BDA as a primary money laundering concern, FinCEN cited in the Federal Register that "the involvement of North Korean Government agencies and front companies in a wide variety of illegal activities, including drug trafficking and the counterfeiting of goods and currency" and noted that North Korea has been positively linked to nearly 50 drug seizures in 20 different countries since

1990. Following an investigation of BDA conducted with the cooperation of the Macau authorities, Treasury finalized the Section 311 rule in March 2007, prohibiting U.S. financial institutions from opening or maintaining correspondent accounts for or on behalf of BDA. This rule remains in effect.

Shortly after the U.S. designation, The Monetary Authority took control of Banco Delta Asia and froze approximately U.S. $25 million in accounts linked to North Korea. The Government of Macau announced in March 2007 that it would continue to maintain control over Banco Delta Asia for at least six more months to resolve the Banco Delta Asia situation. In April, 2007, the Macau authorities released the $25 million North Korean-related funds frozen at BDA. In September 2007, The Treasury Department's Financial Crimes Enforcement Network denied two petitions filed on behalf of BDA and its owners to lift the Section 311 Final Rule designating BDA as a "primary money laundering concern." On September 30, 2007, Macau Monetary Authority announced that Banco Delta Asia would be returned immediately to its shareholders, but continued international restrictions on BDA and its subsidiaries outside of Macau that limit BDA to pataca currency business in Macau. Those restrictions remain in place.

In December 2006, the Asia Pacific Group (APG) and Offshore Group of Banking Supervisors (OGBS) conducted a joint Mutual Evaluation of anti-money laundering and combating financing of terrorism measures in place in Macau. The Mutual Evaluation Report stated that Macau was noncompliant with FATF Special Recommendation IX, and encouraged Macau to enact measures to detect the physical cross border transport of currency and bearer-negotiable instruments. Macau does not require reporting of the movement of currency above any threshold level across its borders, or reporting of large currency transactions above any threshold level.

Macau's AML/CTF regime was also rated as deficient in a number of other respects, including: the lack of a mechanism to confiscate, freeze, and forfeit proceeds of crime independent of criminal process; the lack of specific ability to freeze terrorist funds; failure to establish an independent and permanent FIU; the lack of requirements for financial institutions to verify the identify the beneficial owners of transactions made by third parties, or to examine the background and purpose of transactions with no economic or visible lawful purpose; the failure to develop a risk assessment of, and risk based approach to the gaming sector; and the lack of adequate legal framework for requiring Designated Non-Financial Business and Professions, including casinos and gaming concessionaires to report suspicious transactions.

Macau should continue to improve its ability to implement and enforce existing laws and regulations. Macau should ensure that regulations, structures, and training are adequate to prevent money laundering in the gaming industry, including implementing and enforcing regulations to prevent money laundering in casinos, especially regulations to improve oversight of VIP rooms. The MSAR should, put in place detection and declaration systems for cross-border bulk currency movement. Macau should establish asset-freezing mechanisms and procedures to fully implement UN Security Council Resolutions 1267 and 1373. This process should not be linked to the criminal process and should include the ability to freeze terrorist assets without delay. Macau should increase public awareness of the money laundering problem, improve interagency coordination and training, and boost cooperation between the MSARG and the private sector in combating money laundering. Macau should institutionalize its Financial Intelligence Unit by making it a permanent, statutory body. Macau should pursue membership in the Egmont Group, and, in the meantime, ensure the FIU meets Egmont Group standards for information sharing. Macau should devote additional resources to compiling data on financial crimes, including money laundering and terrorist financing, and make that information available to appropriate partners. Macau's Judicial Police have limited resources devoted to AML/CTF investigations. Additional manpower would allow for more investigations and enforcement action.

Malaysia

Malaysia is a growing regional financial center vulnerable to money laundering. Malaysia has developed an anti-money laundering and counterterrorist finance (AML/CTF) framework based on the country's Anti-Money Laundering and Anti-Terrorism Financing Act (AMLATFA). Malaysia's has long porous land and sea borders and its strategic geographic position influence money laundering and terrorist finance in the region. Drug trafficking is the main source of illegal proceeds in Malaysia. Malaysia is primarily used as a transit country to transfer drugs originating from the Golden Triangle and Europe, which among others, include heroin, amphetamine type substances and ketamine. Other sources of illegal proceeds include corruption, theft, fraud, smuggling, forgery, and illegal gambling. Money laundering techniques include the use of front companies, purchasing high value goods and real property, investment in capital markets, and the use of money changers. Smuggling of goods subject to high tariffs is a source of illicit funds. Malaysia still has a significant informal remittance sector; however, Bank Negara Malaysia (BNM), the Central Bank, actively promotes the migration of informal remittance channels to the formal channels.

Malaysia's National Coordination Committee to Counter Money Laundering (NCC), comprised of members from 15 government agencies, is responsible for the development of the national AML/CTF program, including the coordination of national-wide AML/CTF efforts.

In February 2007, the Asia/Pacific Group on Money Laundering (APG) conducted its second Mutual Evaluation on Malaysia. The evaluation was based on all FATF recommendations. Malaysia's AML/CTF regime was found to be in compliance with the majority of the FATF's Forty Plus Nine Recommendations. Malaysia was found "noncompliant" with Special Recommendation on Terrorist Financing IX on cash couriers—a serious deficiency in view of Malaysia's long and porous borders. In addition, the evaluation identified a number of deficiencies specific to Malaysia's offshore banking center on the island of Labuan, including insufficient resources committed to AML/CTF compliance and constraints on the powers of Labuan's financial authority to both access and share bank customer information.

Subsequent to the second mutual evaluation, the NCC established a task force comprised of the Royal Malaysian Customs, Immigration Department, Home Ministry, and Bank Negara Malaysia to develop and implement national policies and measures to address physical cross-border transportation of currency and bearer negotiable instruments in line with Special Recommendation IX. This initiative is intended to improve Malaysia's relatively lax customs inspection at ports of entry, particularly along the east coast of Sabah in Borneo where extensive coastlines increase its vulnerability to smuggling, including cash smuggling.

The AMLATFA provides for the establishment of a financial intelligence unit (FIU) in Malaysia. The FIU was established in 2001 within the Central Bank. The FIU is tasked with receiving and analyzing information and sharing financial intelligence with the appropriate enforcement agencies for further investigation. The FIU cooperates with other relevant agencies to identify and investigate suspicious transactions. A comprehensive supervisory framework has been implemented to supervise financial institutions' compliance with the AMLATFA and its subsidiary legislation and relevant guidelines. Currently, BNM maintains 365 examiners who supervise the financial institutions under its purview.

Under the AMLATFA, reporting institutions cover a wide range of institutions, including financial institutions from the conventional, Islamic, and offshore sectors, offshore listing sponsors and trading agents, stock brokers, futures brokers, unit trust management companies, fund managers, futures fund managers, money lenders and pawnbrokers, nonbank remittance service providers, nonbank affiliated charge and credit card issuers, insurance financial advisers, e-money issuers and leasing and factoring businesses, as well as nonfinancial businesses and professions including lawyers, notaries public, accountants, company secretaries, licensed casinos, licensed gaming outlets, registered estate agents, trust companies and dealers in precious metals and precious stones.

These reporting institutions are subject to strict customer due diligence (CDD) rules under the AMLATFA. Every transaction, regardless of its size, is recorded. Reporting institutions must maintain records for at least six years and promptly report any suspicious transactions to the FIU, regardless of the amount of transaction. In addition, a cash threshold reporting (CTR) requirement above RM 50,000 (approximately $14,000) was imposed upon banking institutions. FIU officials indicate that they receive regular reports from the AMLATFA reporting institutions. Reporting individuals and their institutions are protected by statute with respect to their reporting and cooperation with law enforcement. While Malaysia's bank secrecy laws prevent general access to financial information, those secrecy provisions are overridden in the case of suspicious transactions reporting, currency transactions reporting, or in relation to criminal investigations.

Despite these robust CDD and reporting requirements, the APG 2007 mutual evaluation assessed Malaysia as only "partially compliant" on Special Recommendation IV covering the obligation to report suspicions of terrorist financing. Malaysia has introduced but not yet enacted amendments to the AMLATFA to address this deficiency.

Malaysia has adopted banker negligence (due diligence) laws that make individual bankers responsible if their institutions launder money or finance terrorists. Both reporting institutions and individuals are required to adopt internal compliance programs to guard against any offense. Under the AMLATFA, any person or group that engages in, attempts to engage in, or abets the commission of money laundering or financing of terrorism is subject to criminal sanction.

All reporting institutions are subject to supervision and examination by the respective supervisory authorities or the FIU. Malaysia has implemented a comprehensive supervisory framework to supervise reporting institutions' compliance with the AMLATFA and its subsidiary legislation as well as the relevant guidelines. Currently, BNM maintains a large pool of examiners who are involved in the supervision of the financial institutions under the purview of BNM, including branches and subsidiaries located in Labuan, Malaysia's offshore financial services center.

Malaysia's growing Islamic finance sector is subject to the same regulatory requirements and supervision to combat financial crime as the conventional banks. As of end September 2008, in terms of market share, the assets of the Islamic banking system constitute 16.6 percent of the total banking assets, up from 12 percent in mid-2007.

In 1998, Malaysia imposed foreign exchange controls that restricted the flow of the local currency from Malaysia. Malaysia progressively liberalized the exchange control policy while pursuing measures to combat AML/CTF effectively. Most recently, rules were amended on October 1, 2007 to require an individual form to be completed for each transfer above RM 200,000 (approximately $56,000). In addition, banks are obligated to record the amount and purpose of transactions ranging between the equivalent of $2,800 and $56,000.

BNM monitors and assesses remittance service providers (RSPs) to facilitate accessible and inexpensive remittance service in an effort to promote the use of these formal channels. Liberalizations and approvals enacted since 2002 have resulted in the establishment of 30 RSPs with more than 800 branches throughout Malaysia. RSPs are subject to the AML/CTF requirements under the AMLATFA and are under the supervision of BNM. The APG's most recent mutual evaluation of Malaysia in 2007 reported that Malaysia features large scale, unregulated remittance channels and that the jurisdiction requires a strategy to support channeling remittances into formal channels. Due to this and other concerns regarding limited implementation of CDD and record keeping requirements for RSPs, the APG assessed Malaysia as "partially compliant" with Special Recommendation VI on alternative remittances.

While Malaysia's offshore financial center on the island of Labuan has different regulations for the establishment and operation of offshore businesses, it is subject to the same AML/CTF laws as those

governing onshore financial service providers. Malaysia's Labuan Offshore Financial Services Authority (LOFSA) is under the authority of the Ministry of Finance and licenses offshore banks, trust companies, and insurance companies and performs background checks before granting an offshore license. LOFSA is responsible for ensuring AML/CTF compliance on Labuan. However, the APG's 2007 mutual evaluation of Malaysia reported that the LOFSA has devoted insufficient resources to this mission.

Labuan's 59 offshore banks (including 10 investment banks), insurance companies, trust companies, trading agents, and listing sponsors are subject to all AML/CTF requirements, including the filing of suspicious transaction reports under the AMLATFA. Through LOFSA, Malaysia is a member of the Offshore Group of Banking Supervisors and works closely with BNM. The financial institutions operating in Labuan are generally among the largest international banks and insurers. Nominee (anonymous) directors are not permitted for offshore banks or for trust or insurance companies. As of October 2008, Labuan has 6,802 registered offshore companies. Bearer instruments are strictly prohibited in Labuan. Offshore companies must be established through a trust company. Trust companies are required by law to establish true beneficial owners and submit suspicious transaction reports. There is no requirement to publish the true identity of the beneficial owner of international corporations; however, LOFSA requires all organizations operating in Labuan to disclose information on its beneficial owner or owners, as part of its procedures for applying for a license to operate as an offshore company. LOFSA maintains financial information on licensed entities, releasing it either with the consent of those entities or upon investigation. In April 2006, LOFSA announced that it had subscribed to a service which provides structured intelligence on high and heightened risk individuals and entities, including terrorists, money launderers, politically exposed persons, arms dealers, sanctioned entities, and others, to gather information on their networks and associates. LOFSA now uses this service as part of its licensing application process. According to the 2007 MER, LOFSA has only one AML/CTF compliance officer—a fact that may explain why the number of STRs that are reported by LOFSA's banks and trust companies are negligible.

The Free Zone Act of 1990 is the enabling legislation for free trade zones in Malaysia. The zones are divided into Free Industrial Zones (FIZ), where manufacturing and assembly takes place, and Free Commercial Zones (FCZ), generally for warehousing commercial stock. The Minister of Finance may designate any suitable area as an FIZ or FCZ. Currently there are 17 FIZs and 17 FCZs in Malaysia. The Minister of Finance may appoint any federal, state, or local government agency or entity as an authority to administer, maintain, and operate any free trade zone. Companies wishing to operate in an FIZ or FCZ must apply for a license and be approved. The time needed to obtain such licenses from the administrative authority to operate in a particular free trade zone depends on the type of activity. Clearance time ranges from two to eight weeks. There is no indication that Malaysia's free industrial and free commercial zones are being used for trade-based money laundering schemes or by the financiers of terrorism. The zones are dominated by large international manufacturers such as Dell and Intel, which are attracted to the zones because they offer preferential tax and tariff treatment.

Malaysia made its first money laundering arrest in 2004. As of October 2008, the Attorney General's Chambers had prosecuted 62 money laundering cases, involving a total of 2,392 charges with a cumulative total of RM 744.98 million ($225.7 million). These money laundering cases include self-laundering cases where the criminals who committed the predicate offences dealt/laundered the proceeds themselves. Out of the 62 cases, there have been four convictions. Most of the other cases are ongoing. In 2008, there were enforcement actions by Bank Negara Malaysia which resulted in advisories to the public to be cautious of investment schemes promoted on the internet, through phone calls or through seminars conducted by individuals or companies that are not licensed or authorized to accept deposits or to conduct foreign currency dealings.

In April 2002, the GOM passed the Mutual Assistance in Criminal Matters Act (MACMA), and in July 2006 concluded a Mutual Legal Assistance Treaty (MLAT) with the United States. The treaty

came into force in January, 2009. Malaysia concluded a similar treaty among like-minded ASEAN member countries in November 2004. In October 2006, Malaysia ratified treaties with China and Australia regarding the provision of mutual assistance in criminal matters. The mutual assistance treaties enable States Parties to assist each other in investigations, prosecutions, and proceedings related to criminal matters, including terrorism, drug-trafficking, fraud, money laundering and human trafficking.

The GOM has cooperated closely with U.S. law enforcement in investigating terrorist-related cases since the signing of a joint declaration to combat international terrorism with the United States in May 2002. In 2007, the GOM improved the relevant legislation, enabling it to comprehensively freeze assets under the UNSRs 1267 and 1373. The Home Ministry has the authority to declare, by way of order published in the Gazette, terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list as designated entities whose properties are to be frozen. To ensure immediate action to freeze assets of designated entities/individuals, the FIU disseminates electronically an updated UN consolidated list as well as orders or circulars to financial institutions. At the same time, the FIU also disseminates information on persons and entities designated unilaterally by other countries, including the United States, to these institutions. Since 2003 Bank Negara Malaysia has issued 43 circulars and nine accounts have been frozen amounting to $76,400. In 2008, an investigation in Canada tracked about $1.6 million from Canada to an account at a Malaysian-incorporated bank in Kuala Lumpur. The account facilitated the transfer of funds to the Liberation Tigers of Tamil Eelam (LTTE), a designated foreign terrorist organization.

A number of terrorist organizations have been active on Malaysian territory, and authorities have taken action against Jemaah Islamiah. Terrorist financing in Malaysia is predominantly carried out using cash and relies on trusted networks. While Malaysia has recently improved the legislative framework to criminalize terrorist financing, there have been no investigations, prosecutions or convictions relating to terrorist financing under this new scheme. The Ministry of Foreign Affairs opened the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT) in August 2003. SEARCCT coordinates courses and seminars on combating terrorism and terrorist finance.

In March 2007, at the initiation of the NCC, Malaysia enacted amendments to five different pieces of legislation: the AMLA (now known as the AMLATFA), the Penal Code, the Subordinate Courts Act, the Courts of Judicature Act, and the Criminal Procedure Code. Predicate offenses for money laundering were expanded from 219 to 223. Moreover, the amendments impose penalties for terrorist acts, allow for the forfeiture of terrorist-related assets, allows for the prosecution of individuals who have provided material support for terrorists, expand the use of wiretaps and other surveillance of terrorist suspects, and permit video testimony in terrorist cases. This enabled Malaysia to accede to the UN Convention for the Suppression of the Financing of Terrorism. To date, Malaysia has not initiated prosecution of any terrorist suspects or supporters using these amended laws, but instead has continued to use the Internal Security Act which allows for detention without trial. Malaysia is also a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption.

The GOM has rules regulating charities and other nonprofit entities. The Registrar of Societies (ROS) is the principal government official who supervises and controls charitable organizations registered as societies, while those registered as companies limited by guarantee fall under the oversight of the Companies Commission of Malaysia, with input from the Inland Revenue Board. The Registrar mandates that every registered society of a charitable nature submits its annual returns, including its financial statements. Should activities deemed suspicious be found, the Registrar may revoke the nonprofit organization's (NPO) registration or file a suspicious transaction report. Registering an NPO as a society can be bureaucratic and time-consuming. One organization reported that getting registered took nine months and required multiple personal interviews to answer questions about its mission and

its methods. Some NPOs reportedly register as a "company limited by guarantee," a quick and inexpensive process requiring capital of approximately 60 cents and audited financial statements

Malaysia's tax law allows a tax credit, which encourages the reporting of contributions, for Zakat (alms) to mosques or registered Islamic charitable organizations. Islamic Zakat contributions can be taken as payroll deductions, increasing transparency and oversight to help prevent the abuse of charitable giving. Non-Muslims also are allowed a similar tax credit for donations to charitable organizations approved under the Income Tax Act.

The Government of Malaysia continues to enhance its cooperation on a regional, multilateral, and international basis. BNM has signed memoranda of understanding (MOUs) on the sharing of financial intelligence with the FIUs of Australia, Indonesia, Thailand, the Philippines, China, the United Kingdom, United States, Japan, Republic of Korea, Sweden, Chile, Sri Lanka, Brunei, Peru, Bangladesh, Canada, and India.

Malaysia is an active member of the Asia/Pacific Group (APG) on Money Laundering, a regional body designed along the lines of the Financial Action Task Force (FATF). As a member of the APG Donor & Provider Group for Technical Assistance Malaysia works with the World Bank, International Monetary Fund, Asian Development Bank, United Nation Counter-Terrorism Committee Executive Directorate, United Nations Office on Drugs and Crime, the Australian FIU (AUSTRAC), and others to provide technical assistance programs in various ASEAN member countries. Currently, Malaysia is working with the United States to help develop an effective FIU in Afghanistan.

In July 2006, Malaysia was selected as the co-chair of the APG Implementation Issues Working Group (IIWG), which is mandated to provide strategic support to members in implementing FATF Forty Plus Nine Recommendations. As a co-chair, Malaysia has helped develop the Strategic Implementation Planning Framework, which aims to provide post-mutual evaluation implementation assistance to jurisdictions.

Since being accepted as an Egmont Group member in 2003, the FIU in has been elected as the Asia Chair for the Egmont Committee for two consecutive terms (2006-2008 and 2008-2010). In this regard, Malaysia participates as co-sponsor for a number of jurisdictions applying for Egmont Group membership as well as representing the Egmont Group in a number of meetings organized by the APG.

The Government of Malaysia should continue its involvement in AML/CTF matters on a regional, multilateral, and international basis. In addition, Malaysia should improve AML/CTF oversight in Labuan and endow LOFSA with sufficient resources to carry out adequate supervision, particularly over its banks, IBCs, and trust companies. Given that cash smuggling is a major method used by terrorist financers to move money in support of their activities, as a priority matter, the task force established under the NCC should continue its efforts to develop and implement national policies and measures to address physical cross border transportation of currency and bearer negotiable instruments in line with the FATF Special Recommendation IX on bulk cash smuggling. BNM also should continue its efforts to encourage the use of formal rather than informal remittances which are not subject to AML/CTF controls and may pose vulnerabilities for misuse for money laundering and terrorist financing. Law enforcement and customs authorities should examine trade based money laundering and invoice manipulation and their relationship to underground finance and informal remittance systems. More effort should be made in identifying, investigating, and prosecuting terror financing.

Mexico

Mexico is a major drug-producing and drug-transit country and is also one of the major conduits for proceeds from illegal drug sales leaving the United States. Proceeds from the illicit drug trade is the

principal source of funds laundered through the Mexican financial system. Other major sources of illegal proceeds being laundered include corruption, kidnapping, trafficking in firearms and persons, and other crimes. The smuggling of bulk shipments of U.S. currency into Mexico and the repatriation of the cash into the United States via couriers, armored vehicles, and wire transfers remain favored methods for laundering drug proceeds. In addition, criminal organizations have established networks with criminal groups based in other countries to facilitate and develop new methods to launder illicit funds.

Investigation of money laundering activities involving the cross-border smuggling of bulk currency derived from drug transactions remains a challenge for U.S. law enforcement officials. Sophisticated and well-organized drug trafficking organizations based in Mexico are able to take advantage of the extensive U.S.-Mexico border and the large flow of legitimate remittances. The combination of a sophisticated financial sector and relatively weak regulatory controls facilitates the concealment and movement of drug proceeds. U.S. officials estimate that since 2003, as much as $22 billion may have been repatriated to Mexico from the United States by drug trafficking organizations. In April 2006, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) issued a warning to the U.S. financial sector on the potential use of certain Mexican financial institutions, including Mexican casas de cambios (licensed foreign exchange offices) and centros cambiarios (unlicensed foreign exchange offices), to facilitate bulk cash smuggling.

Corruption is also of concern: in the last year, various Mexican government officials have come under investigation for alleged corruption and money laundering activities. The Government of Mexico (GOM) took on internal corruption in 2008 and launched a "cleaning operation" aimed at ending corruption inside its enforcement agencies, including the Office of the Attorney General—Special Unit for Organized Crime (PGR-SIEDO), the Secretariat for Public Security (SPP), the Federal Preventive Police (PFP), and the Federal Investigative Agency (AFI). In November 2008, PGR agents apprehended the former Deputy Attorney General of SIEDO. To date, eight enforcement agents from PFP and PGR have been apprehended and accused of leaking confidential information to drug cartels.

In January 2008, the International Monetary Fund (IMF) conducted a mutual evaluation of Mexico on behalf of the Financial Action Task Force (FATF). The evaluation noted improvements to the GOM's AML/CTF regime and identified deficiencies, including a lack of criminal liability for legal persons and a lack of investigations for money laundering and cross-border cash smuggling.

In 2000, Mexico amended its Customs Law to reduce the threshold for reporting inbound cross-border transportation of currency or monetary instruments from $20,000 to $10,000. At the same time, it established a requirement for the reporting of outbound cross-border transportation of currency or monetary instruments valued at $10,000 or greater. Customs authorities send these reports to the financial intelligence unit (FIU) and cover a wide range of monetary instruments including bank drafts. As a result of the cooperation between Mexican Customs, the Financial Crimes Unit of the Office of the Deputy Attorney General against Organized Crimes (SIEDO), and various U.S. agencies, Mexico has seized over $60 million in bulk currency shipments leaving Mexico City's international airport since 2002. As of November 2008, bulk-cash seizures amount to $53 billion.

Currently, there are 46 banks including 6 development banks and 71 foreign financial representative offices operating in Mexico, as well as 95 insurance companies, 479 investment companies, 155 credit unions, and 24 casas de cambio. The number of casas de cambio will likely decline due to actions the Mexican authorities have taken against those with serious AML/CTF violations and the closure of correspondent accounts in the United States. Commercial banks, foreign exchange companies, and general commercial establishments may offer money exchange services. The Ministry of the Interior (SEGOB) issues temporary licenses for national lotteries, casinos, horse races, and sport pools, but these operations as well as lawyers, accountants, real estate agents, dealers of precious metals and stones, and couriers are currently not subject to anti-money laundering reporting requirements.

Although the underground economy is estimated to account for 20-40 percent of Mexico's gross domestic product, the informality of that economy is considered to be much less significant with regard to money laundering than the criminally-driven segments of the economy.

From 2000 to 2007, inbound remittances grew from $6.6 billion to $24 billion a year. However, remittances have declined by 3.7 percent from January through September 2008 compared with the same period in 2007. Many U.S. banks have partnered with their Mexican counterparts to develop systems to simplify and expedite the transfer of money, including wider acceptance by U.S. banks of the matricula consular, an identification card issued by Mexican consular offices to Mexican citizens residing in the United States that has been criticized as insecure. In some cases, the sender or the recipient can simply provide his/her matricula consular as identification to execute a remittance, often without having to open a bank account. While this makes licit remittances more accessible, it also leaves the system open to potential money laundering and exploitation by organized crime groups. In 2007, electronic transfers accounted for 95 percent of all remittances to Mexico. It is likely that few first-tier commercial banks will reach down to serve low-income clients who receive such remittances, with cajas populares and cajas solidarias (financial cooperatives that function as credit unions) as the likely candidates to fill this gap. This presents a new set of concerns over whether this system will present potential money laundering opportunities for bulk currency transactions.

The Tax Code and Article 400 bis of the Federal Penal Code criminalize money laundering related to any serious crime. Mexico's all-crimes approach to money laundering criminalizes the laundering of the proceeds of any intentional act or omission, regardless of whether or not that act or omission carries a prison term. Rather than applying to proceeds of criminal offenses, the statute applies to "the proceeds of an illicit activity", which is defined as resources, rights, or goods of any nature for which there exists well-founded certainty that they are derived directly or indirectly from or represent the earnings derived from the commission of any crime, and for which no legitimate origin can be established. Money laundering is punishable by imprisonment of five to fifteen years and a fine. Penalties increase when a government official in charge of the prevention, investigation, or prosecution of money laundering commits the offense. This construction of the predicate offense allows prosecutors, upon demonstrating criminality, to shift the burden of proof to the defendant to establish the legitimate origin of the property. An offense committed outside of Mexico may also constitute a predicate offense for money laundering. Because criminal proceeds generated abroad would have an effect in Mexico when laundered in or through its national territory, the laundering of those proceeds could be prosecuted under Mexican law.

Four supervisory agencies are responsible for the compliance with AML/CTF requirements. For AML/CTF purposes, there are four main supervisory agencies: the National Banking and Securities Commission (CNBV), the National Insurance and Bonds Commission (CNSF), the National Retirement Savings System Commission (CONSAR), and the Tax Administration Service (SAT). The CNBV regulates and supervises banks, limited scope financial companies, securities brokerage firms, foreign exchange firms, and mutual funds and subscribes to a risk-based approach to supervision. The CNBV also has the remit to impose administrative sanctions for noncompliance, revoke licenses, and conduct on-site inspections and off-site monitoring of regulated entities. The SAT supervises centros cambiarios (nonlicensed foreign exchange retail centers), money remitters, and unregulated sofomes (multiple purpose financial companies). A 2005 provision of the tax law requires real estate brokerages, attorney, notaries, accountants, and dealers in precious metals and stones to report all transactions exceeding $10,000 to the SAT, which shares the information with the FIU. According to the SAT, there are 882 registered money transmitters and 4380 unlicensed centros cambiarios. In 2006, nonprofit organizations were made subject to reporting requirements for donations greater than $10,000.

The Ministry of Finance, through the Banking, Securities and Savings Unit (UBVA), is responsible for issuing regulations and criteria to interpret anti-money laundering (AML) regulations. Regulations

require banks and other financial institutions (including mutual savings companies, insurance companies, securities brokers, retirement and investment funds, financial leasing and factoring funds, casas de cambio, and centros cambiarios to conduct customer due diligence. The regulations impose customer identification requirements on a range of categories of clients which includes legal persons, individuals, beneficiary owner information and specific provisions for nationals and foreigners. Regulations require enhanced due diligence for higher-risk customers including politically exposed persons. Banks also require identification of occasional customers performing transactions equivalent to or exceeding $500 in value, so that banks can aggregate the transactions daily to prevent circumvention of cash transaction reports (CTRs) and suspicious transaction reports (STRs) filing requirements. Institutions must maintain records of transactions for a period of ten years. Financial institutions have also implemented programs for screening new employees and verifying the character and qualifications of their board members and high-ranking officers. These institutions have also implemented regular training for their employees on money laundering. With regard to wire transfers, financial institutions are required to obtain originator information. However, the threshold for identification of occasional customers is $3,000 and does not include the obligation to aggregate lower transactions for a single customer over a period of time. No guidelines have been issued to assist financial institutions with meeting this obligation. In addition, money remitters are not subject to wire transfer regulations.

The UBVA drafted a multifaceted reform which is under review by the Improvement Regulatory Commission (COFEMER), and observers expect approval in early 2009. The reform, when effective, will harmonize the rules and standards between larger banks and other smaller financial institutions such as credit unions, centros cambiarios, and sofoles (limited purpose lending companies) undergoing deregulation and transitioning to sofomes. Sofomes can be subject to or exempt from regulation depending upon their financial activities. The CNBV will supervise the regulated sofomes that maintain a financial relationship with credit institutions and controlling companies of financial groups, and the SAT will supervise the unregulated sofomes. There are currently 13 regulated sofomes and 634 unregulated sofomes. There are no AML/CTF regulations and supervision has not commenced for these institutions as of yet.

The UBVA draft reform also includes regulations for prepaid cards and travelers checks. The government will provide banks and other financial entities the authority to exchange information among themselves regarding money laundering and terrorist financing without violating bank secrecy provisions. The new regulations will require entities to provide more details, such as complete address and other relevant information in the reports submitted to the FIU. The implementing rules will also include a specific definition between “user” (for remittances, casas de cambio, and centros cambiarios) and “customer” (a person who signs a contract or has a bank account).

When implemented, the reform will reduce the threshold to identify a user of cash operations, travelers checks or prepaid cards from $3,000 to $500. For operations larger than $3,000, the reform will require foreign exchange houses, centros cambiarios, and money transmitters to create a complete file of the user. Financial institutions will need to monitor and identify operations in pesos using a threshold of 300,000 pesos (approximately $21,600) for individuals and 500,000 pesos (approximately $36,000) for companies; formerly, institutions conducted such monitoring exclusively in dollars. To improve the detection of money laundering, financial entities will have 30 days to report fractioned operations exceeding $10,000. The reform will also enable Mexico to identify those sectors that do not comply with money laundering preventive measures.

In 2004, the Ministry of the Treasury (SHCP) reorganized and renamed its financial intelligence unit (FIU), the Unidad de Inteligencia Financiera (UIF). The UIF has approximately 70 staff, but officials expect this number to increase to 150 next year. Forensic accountants, lawyers, and analysts comprise the majority of FIU staff. Regulated entities must report to the UIF any suspicious transactions, currency transactions over $10,000 (except for centros cambiarios, which are subject to a $3,000

threshold), and transactions involving employees of financial institutions who engage in suspicious activity.

The UIF is responsible for receiving, analyzing, and disseminating STRs and CTRs, as well as reports on the cross-border movements of currency. In 2008, UIF received 36,934 STRs and 6,513,147 CTRs. Following the analysis of the reports, the UIF sends reports that are deemed to merit further investigation, and have been approved by the SHCP's legal counsel, to the PGR. The UIF sends an average of 60 cases per month to the PGR for its consideration for prosecution. The PGR's special financial crimes unit (within SIEDO) works closely with the UIF in money laundering investigations. UIF personnel also have working-level relationships with other federal law enforcement entities, including the Federal Investigative Agency (AFI) and the Federal Police (PFP), to help it support the PGR's investigations of criminal activities with ties to money laundering. From 2004 through 2007, 17 criminals have been convicted of money laundering, and $4.5 billion have been seized by the PGR's financial crimes unit. The UIF also reviews all crimes linked to Mexico's financial system and examines the financial activities of public officials. In 2007 and 2008, U.S. authorities observed a significant increase in the number of complex money laundering investigations by SIEDO, with support from the UIF and in coordination with U.S. officials. The number of investigations rose from 152 in 2004 to 198 as of October 2008. In 2007, 85 of 112 apprehension orders corresponded to money laundering operations.

The PGR's special financial crimes unit is understaffed. The lack of personnel—including more field investigators, prosecutors, and auditors- monetary resources, a comprehensive and modern database, technological equipment, as well as the vulnerability of its facilities undermine the unit's efforts. Of the estimated $10 billion circulating illegally in the banking system, the PGR is only able to attack one percent of this amount. During the past three months the unit was able to seize between $60 and $70 million. So far, efforts have targeted only key states, such as Tamaulipas, Sinaloa, Nuevo Leon, Mexico City, and Jalisco, but the PGR believes there is reason to refocus on other regions such as the southern states of Quintana Roo and Yucatan, where authorities have detected large movements of illicit resources.

In 2006, the UIF signed Memoranda of Understanding (MOUs) with the Economy Secretariat and the Mexican immigration authorities that provides access to their databases. The UIF has also signed agreements with the CNBV and the National Commission of Insurance and Finance (CNSF) to coordinate to prevent money laundering and terrorist financing. The UIF is currently finalizing similar negotiations with the SHCP and the National Savings Commission (CONSAR).

At the end of 2008, the GOM enacted legislation to reorganize Mexico's law enforcement agencies that attempts to create synergy among the different levels of local, state, and federal law enforcement agencies to combat drug cartels and other organized crime groups. The law will create a National Public Safety Council (to provide assistance to victims of crime, bolster law enforcement institutions, and evaluate the effectiveness of public safety programs) and a National Intelligence Center.

Agencies involved in AML/CTF efforts are currently drafting an AML/CTF National Strategy, anticipated to be issued in 2009. The Strategy will outline Mexico's AML/CTF short and long range objectives and the strategies that the GOM will implement to meet them. It will also establish an interagency coordination group which will examine emerging money laundering trends and identify and propose legal and regulatory measures to mitigate gaps. In August 2008, the GOM approved an Integral Strategy Against Organized Crime. The strategy focuses on the isolation, neutralization, and ultimate disbandment of organized crime through the abolition of their operational, logistical, commercial and financial networks.

There have been a number of noteworthy cases in 2008. In the beginning of 2008, the U.S. Government froze funds belonging to the Mexican money exchange house Casa de Cambio Puebla as part of a money laundering case filed in U.S. District Court in Miami against Venezuelan national

Pedro Jose Benavides Natera, who participated in a complex money laundering scheme. Criminals used clean funds to purchase high-performance turbo-prop aircraft for drug smuggling operations. Drug proceeds from Venezuela were sent to Casa de Cambio Puebla where cooperating individuals sent the funds on to the U.S., into buffer accounts, operated by individuals who served as fronts for Venezuelan drug traffickers. The buffer account holders then transferred funds to aircraft brokers for the purchase of aircraft. The criminals then cancelled the aircraft registrations and had the aircraft shipped to front men in Venezuela.

In October 2008, at a mansion in Desierto de los Leones near Mexico City, PGR and PFP apprehended 15 major drug dealers and money launderers, 11 of them Colombians, with links to the Beltran Leyva brothers. The leader of the group, Teodoro Mauricio aka "El Gaviota", is under investigation for money laundering and narcotics trafficking. These apprehensions are part of an ongoing investigation initiated in 2005 of a group of Colombian traffickers in Mexico linked to the Cali-based Norte Valle Cartel.

In November 2008, SIEDO arrested Jaime Gonzalez Duran, aka "The Hummer", one of the most wanted criminals in Mexico and allegedly one of the leaders and founders of the criminal group "Los Zetas" (considered to be the armed branch of the Gulf Cartel). Gonzalez was apprehended in Reynosa, Tamaulipas where he had smuggled drugs into the U.S., on organized crime, drug smuggling, money laundering, and possession of weapons charges.

Mexico has asset forfeiture laws and provisions for seizing assets abroad derived from criminal activity, and U.S. requests to Mexico for the seizure, forfeiture, and repatriation of criminal assets have occasionally met with success. Mexico does not have a civil forfeiture regime and can only forfeit assets upon a final criminal conviction; it can also seize assets administratively if they are deemed to be "abandoned" or unclaimed. However, draft legislation pending in the Mexican Congress includes constitutional changes that would enable a forfeiture regime similar to Colombia's law of extinguishment of ownership (extinción de dominio). The legislation would provide for seizing and forfeiting assets used by organized criminals in executing drug trafficking, money laundering, kidnapping, car robbery, embezzlement, and trafficking of persons. Currently, these assets remain untouched by enforcement authorities and the state even when criminals are convicted and sentenced to prison. The legislation would permit specialized judges to authorize an asset forfeiture procedure independently of the criminal process being followed against an alleged criminal, and before a final ruling or conviction. Prosecutors from the Attorney General's Office would have access to financial, tax, and real estate information through the CNBV, SAT, and notaries. For assets marked for seizure and forfeiture located abroad, Mexico would request international legal assistance under international treaties and reciprocal cooperation mechanisms. The law would also include sanctions against individuals leasing or renting an asset or property to organized crime with the knowledge that it will be used to commit illegal acts.

Senators amended a Presidential proposal to prevent corruption and abuse of power by PGR prosecutors. In addition to that proposal, there are also Senatorial initiatives. One proposes that forfeited assets be included in a fund to prevent and pursue felonies and organized crime. The Service for the Administration of Forfeited Assets would allocate resources to the corresponding authorities and to cover damages to the victims. The three major political parties are discussing the initiatives with the intention of to achieving consensus and approving the law in early 2009. Mexico City's local congress drafted a similar extincion de dominio law, which was approved at the end of November 2008.

In 2007, Mexico criminalized terrorist financing, with punishments of up to 40 years in prison. The law amends the Federal Penal Code to link terrorist financing to money laundering and establish international terrorism as a predicate crime when it is committed in Mexico to inflict damage on a foreign state. The law also imposes sanctions against an individual or individuals who conceal a

terrorist or a person who threatens to commit a terrorist act. The UBVA distributes the list of individuals and entities that have been included in the UN 1267 Sanction Committee's consolidated list to other government agencies and to financial institutions through the CNBV. The GOM has responded positively to international and USG efforts to identify and block terrorist-related funds, and it continues to monitor suspicious financial transactions, although no such assets have been frozen to date.

Mexico has developed a broad network of bilateral agreements and its law enforcement authorities regularly meet in bilateral law enforcement working groups with their U.S. counterparts. The U.S.-Mexico Mutual Legal Assistance Treaty (MLAT) entered into force in 1991. Mexico and the United States also implement other bilateral treaties and agreements for cooperation in law enforcement issues, including the Financial Information Exchange Agreement (FIEA) and the Memorandum of Understanding (MOU) for the exchange of information on the cross-border movement of currency and monetary instruments.

Mexico is a party to the 1988 UN Drug Convention; the UN Convention against Transnational Organized Crime; the UN Convention against Corruption; and the UN Convention for the Suppression of the Financing of Terrorism. Mexico is a member of the FATF and the Financial Action Task Force for South America (GAFISUD), a FATF-style regional body, of which Mexico currently holds the presidency. In addition to its membership in the FATF and GAFISUD, Mexico participates in another FATF-style regional body, the Caribbean Financial Action Task Force (CFATF), as a cooperating and supporting nation. The UIF is a member of the Egmont Group of Financial Intelligence Units.

The Government of Mexico (GOM) has made fighting money laundering and drug trafficking one of its top priorities, and has made substantial progress in combating these crimes over the course of 2008. However, Mexico continues to face challenges with respect to is anti-money laundering and counterterrorist financing regime, particularly with its ability to prosecute and convict money launderers.. The GOM should amend its legislation to ensure that legal persons can be held criminally liable for money laundering and terrorism financing. Mexico should also amend its terrorist financing legislation to fully comport with the UN Convention for the Suppression of Terrorist Financing; and enact legislation and procedures to freeze terrorist assets of those designated by the UN Al-Qaida and Taliban Sanctions Committee. To create a more effective regime, Mexico should fully implement and improve its mechanisms for asset forfeiture, control the bulk smuggling of currency across its borders, monitor remittance systems for possible exploitation, improve the regulation and supervision of money transmitters, unlicensed currency exchange centers, centros de cambiarios and gambling centers, and extend AML/CTF requirements to designated nonfinancial businesses and professions.

Moldova

Moldova is not considered an important regional financial center. The Government of Moldova (GOM) monitors money flows through "right-bank" Moldova (the territory it controls), but does not exercise control over the breakaway region of Transnistria. Though unrecognized, Transnistria is a de facto independent region located along the Dniester River between Moldova and Ukraine. Transnistrian authorities do not submit to GOM financial controls and maintain an independent banking system not licensed by the National Bank of Moldova (NBM). Moldovan per capita incomes are the lowest in Europe. Criminal proceeds laundered in Moldova derive primarily from tax evasion, contraband smuggling, foreign criminal activity, and, to a lesser extent, domestic criminal activity and corruption. Human trafficking also may be a source of proceeds laundered in Moldova. Money laundering proceeds are controlled by small, poorly-organized domestic criminal groups. These small groups are, in turn, supervised by larger and better-organized foreign crime syndicates from Russia, Ukraine, Turkey and Israel, among others.

Money laundering has occurred in the banking system and through exchange houses in Moldova; and in the offshore financial centers and throughout the region in Transnistria. The amount of money laundering occurring via alternative remittance systems reportedly is not significant. The number of financial crimes unrelated to money laundering, such as bank fraud, embezzlement, corruption, and forgery of bankcards, especially through international offshore zones, has decreased. Criminal cases in 2008 involved the forgery and misuse of bankcards. Although the number of financial crimes has not increased, investigations have revealed a diversification of financial and economic-related crimes.

Although a significant black market exists in Moldova, especially smuggling of goods at the Moldovan-Ukrainian border alongside Transnistria, narcotics proceeds are not a significant funding source of this market. Contraband smuggling generates funds that are laundered through the banking system. Often funds are first laundered through Transnistrian banks, transferred to Moldovan institutions, and then moved to other countries.

Moldova is not considered an offshore financial center. The Moldovan financial system has 16 banks, including five banks fully or majority-owned by foreigners, that are regulated in the same manner as Moldovan commercial banks. Offshore banks are not permitted to operate in Moldova. Shell companies are not allowed by law, although they exist on a de facto basis. Nominee directors and trustees are prohibited. Internet gaming sites exist, although no statistics are currently available on the number of sites in operation. Internet gaming is subject to the same regulations as domestic casinos. Currently six casinos, two national lottery companies and four sport gambling facilities are licensed and legally operating.

Moldova currently has six free trade zones (FTZs), some of which are infrequently used. Goods from abroad are imported to the FTZs and resold without payment of customs duties to the country of origin or to Moldova. The goods are then exported to other countries with documentation indicating Moldovan origin. According to Moldova's financial intelligence unit (FIU), the Service for Preventing and Combating Money Laundering and Terrorism Financing (SPCSB), through September 30, 2008, no reports have been filed alleging the FTZs have been used in trade-based money laundering schemes or for terrorist financing. A GOM agency, the Free Trade Zone Administration (FTZA), supervises the FTZs. Companies operating in FTZs also are subject to inspections, controls, and investigations by inspectors from the Customs Service and the Center for Combating Economic Crime and Corruption (CCECC).

Money laundering is a separate criminal offense under Article 243 of the Moldovan Criminal Code and under the Law on Preventing and Combating Money Laundering and Terrorism No.190-XVI, (the AML/CTF Law), passed on July 26, 2007. The legislation takes an "all serious crimes" approach. Serious crimes are defined as those punishable by a fine of 500 to 1,000 conventional units (approximately $1,000 to $1,900) or by imprisonment of up to five years. The fine or imprisonment may be accompanied by a prohibition to hold certain positions or to practice a certain activity for a period of two to five years.

In early 2007, the President proposed draft amendments to the tax code and other financial regulations aimed at "liberalizing the economy." On April 27, the Parliament adopted tax-code amendments intended to regulate Moldova's informal economy, forgive tax debts and stimulate investments. Of particular concern was a capital-amnesty provision allowing individuals and legal entities to legalize previously undeclared cash and noncash assets, including real estate and stocks. Additionally, those taking advantage of the amnesty would be under no obligation to declare the origins of their declared assets. The law also stipulates that transaction information can not be shared with the CCECC or the Moldovan Tax Inspectorate. Most worrisome, the legislation exempts declared assets from Moldova's fiscal, customs and existing money laundering and terrorist financing legislation.

Following recommendations from the international community, on July 20, 2007, the Moldovan Parliament adopted Law 2298, a package of tax-code reforms, which includes amendments to the

capital-amnesty law. The amendment closes loopholes in the capital-amnesty law, eliminating explicitly the exemption of amnesty-related transactions from Moldova's anti-money laundering laws. A week later, Parliament separately adopted the new AML/CTF Law. Since the passage of these laws, GOM authorities have issued numerous regulations, decisions, and laws that are related to the tax-amnesty/capital-legalization law and the AML/CTF Law. On August 15, 2007, the NBM issued two decisions focusing on the activity of financial institutions related to capital legalization and the transfer or export from the Republic of Moldova of legalized funds by individuals.

Article 12 of the AML/CTF Law regulates the limitations of bank secrecy. Thus, information obtained from reporting entities can be used only with the purpose of preventing money laundering and terrorist financing. The forwarding of information regarding clients or ownership information to the CCECC, criminal investigative authorities, prosecutorial entities, or to the courts in an effort to prevent or combat money laundering activities is not classified as disclosure of commercial bank or professional secrets, as long as the forwarding of information is carried out in accordance with legal provisions.

The CCECC, which has the authority to investigate money laundering and terrorist financing, supervises and examines all banks and nonbanking financial institutions for compliance with anti-money laundering/counterterrorist financing (AML/CTF) laws and regulations. Under the AML/CTF Law, the NBM supervises banks, exchange houses, and representatives of foreign banks. A July 2007 amendment to Law No. 192, on the Securities Commission, merges into one agency, the National Commission on Financial Markets (NCFM), three institutions dealing with oversight of financial markets—the National Commission on Securities, the Inspectorate for Supervision of Insurance Companies and Retirement Funds, and the National Service for Supervision of Citizen's Savings and Lending Associations. The NCFM's jurisdiction includes nonbanking financial entities, such as institutions issuing securities, investors, the National Bureau of Insurance of Vehicles of Moldova, members of saving and lending associations, and clients of micro-financing organizations. Additionally, the NCFM oversees professional participants in the nonbanking financial sector that carry out activities in the following fields: the securities market, insurance market, micro-financing, private pension funds, mortgage organizations, and credit-history bureaus. The Licensing Chamber checks the compliance of companies applying for business licenses, and specifically oversees casinos and gaming facilities.

Banks, exchange houses, stock brokerages, casinos, insurance companies, lawyers, notaries, accountants, lotteries, and institutions organizing or displaying lotteries are required to record and report the identity of customers engaging in significant transactions. The reporting entities are obligated to report suspicious transactions to the FIU within 24 hours. In addition, single transactions or multiple transactions undertaken in 30 calendar days that exceed MDL 500,000 (approximately $50,000) must be reported to the FIU. The AML/CTF Law also requires financial institutions to maintain records and documentation (including business correspondence) of accounts and account holders for a period of at least seven years after the termination of business relations or the closing of the account.

The SPCSB, Moldova's FIU, is a quasi-independent unit within the CCECC. Decree No. 111 of September 15, 2003, establishes the SPCSB as a law enforcement style FIU, with multiple responsibilities, including the collection, administration, and analysis of transaction reports. It also conducts criminal investigations and has regulatory authority to develop draft laws. During 2008, the FIU's staff increased by five additional employees, expanding the staff to 19 inspectors. The director of the FIU reports the unit is now better staffed, with 25 employees being an eventual long-term staffing goal. FIU staff went through extensive training in 2008. Although housed within the CCECC building, a secure door separates its offices from other CCECC employees. The heads of the FIU and the CCECC maintain that other CCECC employees have no access to records collected by the FIU. However, the leadership of the FIU is ultimately under the supervision of the director of the CCECC. Since the FIU has become a member of the Egmont Group, the CCECC has allotted additional funds

for upgrading and enhancing FIU facilities as well as for training its staff. While the CCECC budget covers the base financial needs of the FIU, the FIU is also supported technically and financially by international organizations. The head of the FIU reports that the unit is adequately staffed, with low turnover, good working conditions and newly renovated offices.

In an attempt to strengthen the capacities of Moldova's FIU, the European Commission and the Council of Europe have been working extensively with the CCECC and the Moldovan FIU. The project, which began in August 2006, is a three year program which has as its specific objective the strengthening of Moldova's anticorruption and AML/CTF regime.

The CCECC and the FIU are the lead agencies responsible for investigating financial crimes, including money laundering. Other agencies that share jurisdiction over the investigation of financial crimes include the Prosecutor General's Office (PGO), the Ministry of Interior (MOI) and the Customs Service. The Security and Intelligence Service (SIS) investigates terrorist financing. The FIU has formed a task force with the PGO, the MOI, the Customs Service, the NBM, the NCFM, the SIS, and the Ministry of Information Development to share information and discuss investigations. The FIU has signed interagency agreements with other agencies and ministries with databases to exchange information. In 2008, the FIU reported it has been granted access to almost all governmental databases and information systems. In 2008, the FIU improved existing mechanisms on exchange of information at the national and international levels.

In the first nine months of 2008, the FIU received reports on approximately five million financial transactions, of which 16,000 were considered suspicious, a substantial but unexplained decrease from the nine million total reports and the 165,199 suspicious reports in 2007. Also, the total number of suspicious transactions is misleading, since GOM officials categorize all transactions involving Transnistria as suspicious. The FIU indicated ten percent—12 percent of the 16,000 suspicious transactions concern Transnistria.

In 2008, the FIU initiated six criminal cases related to financial fraud; none of these cases carried direct money laundering charges. The FIU identified two major types of criminal activity in 2006 and 2007: in the first instance, criminals used financial transactions that appeared to be legitimate to launder criminal proceeds; and, in the second instance, criminals used the FTZs to create illegal profits by reducing the value of imported goods. In the first nine months of 2008, the FIU imposed fines and sanctions totaling $300,000. The FIU reports there were no arrests of individuals for money laundering violations during the first nine months of 2008. Late in 2007, a Moldovan court tried a criminal case charging the defendant with money laundering violations. The defendant was found guilty and sentenced to 15 years' imprisonment. In 2008, the FIU and CCECC had made no arrests nor pursued any prosecutions involving terrorist financing. Based on the volume of reports received by the FIU, the number of arrests and prosecutions appears to be very low. No explanation was provided for the lack of prosecutions and convictions.

Law No. 1569 of December 2002, on the transportation of currency, stipulates that persons are obliged to report in writing to Moldovan customs officials the amount of currency they are transporting when that amount exceeds 10,000 euros (approximately $13,500). If the amount of outbound currency is more than 10,000 euros (approximately $13,500), the carrier of the currency has to report the outbound currency in a special declaration form provided by customs officials at the border. In addition to the special declaration, the currency carrier must provide documents detailing the source of the money and a special permission for outbound cash currency transportation issued by a duly authorized bank or the NBM. The Customs Service operates a special database that includes all declarations which is shared with other governmental agencies, including the FIU.

The Moldovan Criminal Code provides for the seizure and confiscation of assets related to all serious crimes, including terrorist financing. The provisions may be applied to goods belonging to persons who knowingly accepted goods acquired illegally, even when the state declines to prosecute.

However, it remains unclear whether asset forfeiture may be invoked against those unwittingly involved in or tied to an illegal activity. If it can be shown that the assets were used in the commission of a crime or result from a crime, they can be confiscated. Legitimate businesses can be seized if they were used to launder drug money, support terrorist activity, or are otherwise related to other criminal proceeds. The Criminal Code allows for civil as well as criminal forfeiture.

The PGO has expressed its willingness to pursue an initiative to amend the Constitution to allow a more effective use of asset forfeiture. The Constitution currently incorporates a presumption that any property owned by an individual was legally acquired. This presumption has acted to inhibit the use of the existing asset forfeiture laws. However, the initiative has not progressed in 2008, likely because both executive and legislative branches have other higher priorities on their agendas.

To the extent of their jurisdictions, the FIU, CCECC, Tax Inspectorate, Customs Service, prosecutor's offices and Bailiff's offices are responsible for tracing, seizing and freezing assets. Assets seized by law enforcement are incorporated into the state budget, not a separate fund. In the first nine months of 2008, the FIU issued decisions freezing and seizing assets totaling MDL 3 million (approximately $300,000).

The banking community generally cooperates with enforcement efforts by the FIU and the CCECC to trace funds and seize or freeze bank accounts. However, the GOM currently lacks adequate resources, training, and experience to trace and seize assets effectively. The GOM does not have a national system for freezing terrorist assets. The GOM has no separate law providing for the sharing with other countries of assets seized from narcotics and other serious crimes. However, nothing in the current legal structure would prohibit such activity.

Article 279 of the Moldovan Criminal Code criminalizes terrorist financing, defining it as a "serious crime." Moldova regulates efforts to combat terrorist financing in the Law on Combating Terrorism, enacted on November 12, 2001. Article 2 defines terrorist financing, and Article 8/1 authorizes suspension of terrorist and terrorist-related financial operations. This statute is separate from the AML/CTF Law, which contains other relevant provisions.

In 2008, the CCECC issued a decree on actions to be taken to enforce the provisions of the AML/CTF Law. The CCECC decree lists entities worthy of particular focus, given possible money laundering or terrorist financing concerns. These entities include countries that may produce narcotics; countries that do not have legal provisions against money laundering and terrorist financing; countries with a high crime rate and corruption; countries operating offshore centers; and persons, groups, and entities identified as participating in terrorist activities. The decree was developed on the basis of Moldova's national interests and U.S. and UN lists of designated terrorists. To date, the Moldovan authorities have not frozen, seized, or forfeited assets related to terrorism or terrorist financing. Reportedly, no indigenous alternative remittance systems exist in Moldova, although the use of cash couriers is common. No special measures have been taken to investigate misuse of charitable or nonprofit entities.

In December 2006, the GOM signed a $24,700,000 Threshold Country Program with the Millennium Challenge Corporation that focuses on anticorruption measures. The GOM requested funding to address areas of persistent corruption including the judiciary, health care system, tax, customs and law enforcement. Moldova is listed as 109 out of 180 countries in Transparency International's 2008 Corruption Perception Index.

The GOM has no bilateral agreement with the United States for the exchange of information regarding money laundering, terrorism, or terrorist financing investigations and proceedings. However, Moldovan authorities continue to solicit USG assistance on individual cases and cooperate with U.S. law enforcement personnel when presented with requests for information or assistance. The FIU has entered into bilateral agreements to exchange information with the FIUs of Albania, Belarus, Bulgaria,

Croatia, Estonia, Georgia, Indonesia, Korea, Lebanon, Lithuania, Macedonia, Netherlands, Romania, Russia, and Ukraine. Moldova has signed an agreement with Commonwealth of Independent States (CIS) member states for the exchange of information on criminal matters, including money laundering.

Moldova is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. On May 20, 2008, the FIU became a member of the Egmont Group. In 2004, the CCECC was accepted as an observer at the Eurasian Group on Combating Money Laundering and Financing of Terrorism, a Financial Action Task Force-style regional body (FSRB). Moldova is a member of the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), a FSRB. Moldova underwent an evaluation by MONEYVAL in 2007. The evaluation was largely unfavorable. Moldova is scheduled to undergo its next MONEYVAL evaluation in 2010.

The Government of Moldova should continue to enhance its existing AML/CTF regime. The GOM should ensure the FIU, law enforcement agencies and prosecutors have sufficient resources, capacity, and tools to adequately analyze and investigate suspected cases of money laundering and terrorist financing. Moldova should improve the mechanisms for sharing information and forfeiting assets, including clarifying if unwitting third parties are subject to the forfeiture provisions. Border and anti-smuggling enforcement should be considered as top priorities in light of the potentially destabilizing effects of continued international organized criminal activity. The GOM should continue the momentum of its anticorruption efforts.

Monaco

The second-smallest country in Europe, the Principality of Monaco is known for its tradition of bank secrecy, network of casinos, and favorable tax regime. Money laundering offenses relate mainly to offenses committed abroad. Russian organized crime and the Italian mafia allegedly have laundered money in Monaco. Reportedly, the Principality does not face ordinary forms of organized crime. Existing crime does not seem to generate significant illegal proceeds, with the exception of fraud and offenses under the "Law on Checks." Monaco remains on an Organization for Economic Cooperation and Development (OECD) list of "noncooperative" countries in terms of provision of tax information.

Monaco has a population of approximately 32,000, of whom fewer than 7,000 are Monegasque nationals. Monaco's approximately 60 banks and financial institutions hold more than 300,000 accounts and manage total assets of about 70 billion euros (approximately $102,800,000,000). Approximately 85 percent of the banking customers are nonresident. The high prices for land throughout the Principality result in a real estate sector of considerable import. There are five casinos run by the Société des Bains de Mer, in which the state holds a majority interest.

The Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), a Financial Action Task Force (FATF)-style regional body, conducted an evaluation of the Monegasque anti-money laundering and counterterrorist financing (AML/CTF) system in 2007. That report identifies a variety of problems with the Monegasque approach, notably with respect to customer due diligence, designated nonfinancial businesses and professions, and the scope of suspicious transaction reporting. These items remain subject to comment.

Money laundering in Monaco is a crime under Act 1.162 of July 7, 1993, "On the Participation of Financial Institutions in the Fight against Money Laundering," and Section 218-3 of the Criminal Code, amended by Act 1.253 of July 12, 2002, "Relating to the Participation of Financial Undertakings in Countering Money Laundering and the Financing of Terrorism." On November 9,

2006, Section 218-3 of the Criminal Code was modified to adopt an "all crimes" approach to money laundering.

Prior approval is required to engage in any economic activity in Monaco, regardless of its nature. The Monegasque authorities issue approvals based on the type of business to be engaged in, the location, and the length of time authorized. This approval is personal and may not be re-assigned. Any change in the terms requires the issuance of a new approval.

Monaco's banking sector is linked to the French banking sector through the Franco-Monegasque Exchange Control Convention, signed in 1945 and supplemented periodically, most recently in 2001. Through this convention, Monaco operates under the banking legislation and regulations issued by the French Banking and Financial Regulations Committee, including Article 57 of France's 1984 law regarding banking secrecy. The majority of entities in Monaco's banking sector concentrate on portfolio management and private banking. Subsidiaries of foreign banks operating in Monaco may withhold customer information from their parent banks.

Although the French Banking Commission supervises Monegasque credit institutions, Monaco shoulders the responsibility for legislating and enforcing measures to counter money laundering and terrorist financing. The Finance Counselor, located within the Government Council, is responsible for AML/CTF policy and program implementation.

Banking laws do not allow anonymous accounts, but the Government of Monaco (GOM) does permit the existence of alias accounts, which allow account owners to use pseudonyms in lieu of their real names. Cashiers do not know the clients, but the banks know the identities of the customers and retain client identification information. Article 8 of Sovereign Order 632 of August 2006 clarifies the circumstances under which pseudonyms can be used by banks.

Monaco's AML legislation, as amended, requires banks, insurance companies, stockbrokers, corporate service providers, portfolio managers, some trustees, and institutions within the offshore sector to report suspicious transactions to Monaco's financial intelligence unit (FIU), and to disclose the identities of those involved. Casino operators must alert the government of suspicious gambling payments possibly derived from drug-trafficking or organized crime. The law imposes a five to ten-year jail sentence for anyone convicted of using illicit funds to purchase property, which itself is subject to confiscation. Act 1.162, as amended, institutes procedural requirements regarding internal compliance, client identification, and retention and maintenance of records. Sovereign Order 16.615 of January 2005 and Sovereign Order 631 of August 2006 mandate additional customer identification measures. Designated nonfinancial businesses and professions, such as lawyers, notaries, accountants, real estate brokers, and dealers in precious metals and stones, are not subject to reporting or record keeping requirements.

Offshore companies are subject to the same due diligence and suspicious transaction reporting (STR) obligations as banking institutions, and Monegasque authorities conduct on-site audits. Act 1.253 strengthens the "know your client" obligations for casinos and obliges companies responsible for the management and administration of foreign entities not only to report suspicions to Monaco's FIU, but also to implement internal AML/CTF procedures. The FIU monitors these activities.

Monaco's FIU, the Service d'Information et de Controle sur les Circuits Financiers (SICCFIN), receives STRs, analyzes them, and forwards them to the prosecutor when they relate to drug-trafficking, organized crime, terrorism, terrorist organizations, or the funding thereof. A 2007 Sovereign Order allows SICCFIN to propose legal or regulatory changes in the areas of money laundering, terrorist financing, and corruption. SICCFIN also supervises the implementation of AML legislation. Under Article 4 of Law 1.162, SICCFIN may suspend a transaction for 12 hours and advise the judicial authorities to investigate. In 2006, SICCFIN received 395 STRs. In 2007, SICCFIN

received 381 STRs, about 55 percent of which were submitted by banks and other financial institutions. SICCFIN received 66 requests for financial information from other FIUs in 2007.

Investigations and prosecutions are handled by the two-officer Money Laundering Unit (Unite de Lutte au Blanchiment) within the police. The Organized Crime Group (Groupe de Repression du Banditisme) may also handle cases. Seven police officers have been designated to work on money laundering cases. Four prosecutions for money laundering have taken place in Monaco, resulting in three convictions.

Monaco's legislation allows for the confiscation of property of illicit origin as well as a percentage of co-mingled illegally acquired and legitimate property. Authorities must obtain a court order to confiscate assets. Confiscation of property related to money laundering is restricted to the offenses listed in the Criminal Code. Authorities have seized assets exceeding 11.7 million euros (approximately $17,000,000) in value as of year-end 2006. Monaco and the United States signed an asset sharing agreement in March 2007.

In July and August 2002, the GOM passed Act 1.253 and promulgated two Sovereign Orders intended to implement UNSCR 1373 by outlawing terrorism and its financing. Monaco passed additional Sovereign Orders in April and August of that year, importing into Monegasque law the obligations of the UN Convention for the Suppression of the Financing of Terrorism. In 2006, Monaco further amended domestic law to implement these obligations. Monaco has not, however, conducted any TF investigations or prosecutions to date.

Monaco has also enacted domestic measures providing a legal basis for the freezing of terrorist funds. While the legal framework, to a certain extent, provides for the imposition of international sanctions and penalties under criminal law in the event of noncompliance, the mechanism does not apply to persons, groups, or entities within the EU. Monaco also lacks specific mechanisms for examining and acting on freezing procedures initiated by other countries.

The Securities Regulatory Commissions of Monaco and France signed a memorandum of understanding (MOU) in March 2002 on the sharing of information between the two bodies. The GOM considers this MOU an important tool to combat financial crime, particularly money laundering.

In November 2008, the GOM hosted a joint meeting of the FATF and MONEYVAL to discuss money laundering and terrorist financing typologies. Monaco characterized this conference as part of the "pro-active policy" implemented over the last few years to combat these activities.

Monaco has concluded 15 extradition treaties with various countries. To date, there have been no extraditions on the grounds of money laundering, although the GOM has extradited criminals guilty of other offenses, mainly to Russia. SICCFIN has signed information exchange agreements with over 20 foreign FIUs.

Monaco is a member of MONEYVAL, and SICCFIN is a member of the Egmont Group. Monaco is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. The GOM has neither signed nor ratified the UN Convention against Corruption.

The Government of Monaco should amend its legislation to implement full corporate criminal liability. The Principality should continue to enhance its AML and confiscation regimes by fully applying its AML/CTF reporting, customer identification, and record keeping requirements to all trustees and gaming houses. More broadly, the GOM should extend AML/CTF regulations to cover designated nonfinancial businesses and professions. SICCFIN should have the authority to forward reports and disseminate information to law enforcement and foreign FIUs even when the report or information obtained does not relate specifically to drug-trafficking, organized crime, or terrorist activity or financing. Monaco should become a party to the UN Convention against Corruption.

Morocco

Morocco is not a regional financial center, but money laundering is a concern due to its narcotics trade, vast informal sector, trafficking in persons, and large level of remittances from Moroccans living abroad. According to the 2008 World Drug Report by the United Nations Office on Drugs and Crime (UNODC), Morocco remains the world's principal producer and exporter of cannabis resin. Credible estimates of Morocco's informal financial sector range between 17 and 40 percent of GDP. In 2007, remittances from Moroccans living abroad increased by 15 percent over their level in 2006, and totaled more than $7 billion, approximately nine percent of GDP. Although the true extent of the money laundering problem in the country is unknown, conditions exist for it to occur.

In the past few years, the Kingdom of Morocco has taken a series of steps to address the problem, most notably the enactment of a comprehensive anti-money laundering (AML) bill in May 2007 and the planned establishment of a Financial Intelligence Unit, expected to become operational in Rabat in early 2009. The predominant use of cash, informal value transfer systems and remittances from abroad all help fuel Morocco's informal sector. Bulk cash smuggling is also a problem. There are unverified reports of trade-based money laundering, including under-and over-invoicing and the purchase of smuggled goods. Most businesses are cash-based with little invoicing or paper trail. Cash-based transactions in connection with cannabis trafficking are of particular concern. According to the UNODC, Morocco remains the world's principal producer of cannabis, with revenues estimated at over $13 billion annually. While some of the narcotics proceeds are laundered in Morocco, most proceeds are thought to be laundered in Europe.

Unregulated money exchanges remain a problem in Morocco and were a prime impetus for Morocco's recent AML legislation. Although the legislation targets previously unregulated cash transfers, the country's vast informal sector creates conditions for this practice to continue. While the Moroccan banking sector is a regional leader, only three in ten Moroccans use banks. The sector consists of 16 banks, five government-owned specialized financial institutions, approximately 30 credit agencies, and 12 leasing companies. The monetary authorities in Morocco are the Ministry of Economy and Finance and the Central Bank—Bank Al Maghrib—that monitors and regulates the banking system. A separate Foreign Exchange Office regulates international transactions.

Since 2003, Morocco has taken a series of steps to tighten its AML controls. In December 2003, the Central Bank issued Memorandum No. 36, in advance of pending AML legislation that instructed banks and other financial institutions under its control to conduct internal analysis and investigations into financial transactions. The measures called for the reporting of suspicious transactions, retention of suspicious activity reports, and mandated "know your customer" procedures. In 2007, Morocco's AML efforts took a significant step forward with parliamentary passage and promulgation of a comprehensive AML law, which draws heavily from FATF recommendations. The law requires the reporting of suspicious financial transactions by all responsible parties, both public and private, who in the exercise of their work, carry out or advise on the movement of funds possibly related to drug trafficking, human trafficking, arms trafficking, corruption, terrorism, tax evasion, or forgery. The Bank al-Maghrib and the Ministry of Economy and Finance embarked on a major campaign to publicize the law in 2007, but delays in promulgating the decrees to implement the legislation meant that the Financial Intelligence Unit (FIU) did not become operational in 2008. The government has set a new goal of January 2009 for establishment of the FIU. There were no prosecutions for money laundering in Morocco in 2008.

Morocco has a free trade zone in Tangier, with customs exemptions for goods manufactured in the zone for export abroad. There have been no reports of trade-based money laundering schemes or terrorist financing activities using the Tangier free zone or the zone's offshore banks, which are regulated by an interagency commission chaired by the Ministry of Finance.

While there have been no verified reports of international or domestic terrorist networks using the Moroccan narcotics trade to finance terrorist organizations and operations in Morocco, investigations into the Ansar Al Mahdi and Al Qaeda in the Islamic Maghreb (AQIM) terrorist organizations are ongoing. At least two suspects arrested as part of the Ansar Al Mahdi cell were accused of providing financing to the cell.

Morocco has a relatively effective system for disseminating United Nations Security Council Resolution (UNSCR) terrorist freeze lists to the financial sector and law enforcement. Morocco has provided detailed and timely reports requested by the UNSCR 1267 Sanctions Committee and some accounts have been administratively frozen. In 1993, a mutual legal assistance treaty between Morocco and the United States entered into force.

Morocco is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. Morocco is a charter member of the Middle East and North Africa Financial Action Task Force (MENAFATF).

In June 2003, Morocco adopted a comprehensive counterterrorism bill. This bill provided the legal basis for lifting bank secrecy to obtain information on suspected terrorists, allowed suspect accounts to be frozen, and permitted the prosecution of terrorist finance-related crimes. The law also provided for the seizure and confiscation of terrorist assets, and called for increased international cooperation with regard to foreign requests for freezing assets of suspected terrorist entities. The counterterrorism law brought Morocco into compliance with UNSCR 1373 requirements for the criminalization of the financing of terrorism. Other AML controls include legislation prohibiting anonymous bank accounts and foreign currency controls that require declarations to be filed when transporting currency across the border. Although Morocco criminalized terror finance (TF) in 2003, according to MENAFATF, "the Moroccan definition of TF is narrow, since it does not criminalize the act of using funds by a terrorist organization or by a terrorist."

The Government of Morocco should continue to implement anti-money laundering/counterterrorist financing (AML/CTF) programs and policies that adhere to world standards, including a viable FIU that receives, analyzes, and disseminates financial intelligence. The informal economy is very significant in Morocco and authorities are likely to face major challenges as the new AML regime is implemented. Police and customs authorities, in particular, should enhance their ability to recognize money laundering methodologies, including trade-based laundering and informal value transfer systems.

The Netherlands

The Netherlands is a major financial center and consequently an attractive venue for laundering funds generated from illicit activities. These activities are often related to the sale of cocaine, cannabis, or synthetic and designer drugs (such as ecstasy). Several Dutch financial institutions engage in international business transactions involving large amounts of United States currency. However, there are no indications that significant amounts of U.S. dollar transactions conducted by financial institutions in the Netherlands stem from illicit activity. Financial fraud is believed to generate a considerable portion of domestic money laundering and there is evidence of trade-based money laundering. There are no indications of syndicate-type structures in organized crime or money laundering, and there is virtually no black market for smuggled goods in the Netherlands. Although under the Schengen Accord there are no formal controls on national borders within the EU, the Dutch authorities run special operations in the border areas with Germany and Belgium to keep smuggling to a minimum. Reportedly, money laundering amounts to 18.5 billion euros (approximately $25,000,000,000) annually, equivalent to three percent of Dutch GDP. The Netherlands is not an offshore financial center nor are there any free trade zones in the Netherlands.

In 1994, the Government of the Netherlands (GON) criminalized money laundering related to all crimes. In December 2001, the GON enacted legislation specifically criminalizing facilitating, encouraging, or engaging in money laundering. This eases the public prosecutor's burden of proof regarding the criminal origins of proceeds: under the law, the public prosecutor only needs to prove that the proceeds "apparently" originated from a crime. This application of the law was confirmed by a Dutch Supreme Court case in 2004. Self-laundering also is covered.

The Netherlands has an "all offenses" regime for predicate offenses of money laundering. The penalty for "deliberate acts" of money laundering is a maximum of four years' imprisonment and a maximum fine of 45,000 euros (approximately $55,400), while "liable acts" of money laundering (by people who do not know first-hand of the criminal nature of the money's origin but should have reason to suspect it) are subject to a maximum imprisonment of one year and a fine no greater than 45,000 euros (approximately $55,400). Habitual money launderers may be punished with a maximum imprisonment of six years and a maximum fine of 45,000 euros (approximately $55,400); and those convicted also may have their professional licenses revoked. In addition to criminal prosecution for money laundering offenses, money laundering suspects also can be charged with participation in a criminal organization (Article 140 of the Penal Code), violations of the financial regulatory acts, violations of the Sanctions Act, or noncompliance with the obligation to declare unusual transactions according to the Economic Offenses Act.

In June 2008, the Netherlands Court of Audit (Algemene Rekenkamer, similar to the U.S. General Accountability Office) published its investigation of the GON's policy for combating money laundering and terrorist financing. The report criticizes the Ministries of Interior, Finance, and Justice for: lack of information sharing among them; too little use of asset seizure powers; limited financial crime expertise and capacity within law enforcement; and light supervision of notaries, lawyers, and accountants. The ministries agreed in large part with these conclusions and are taking steps to address them.

The GON's 2008 "National Threat Assessment on Organized Crime," submitted to Parliament in November 2008, concludes that the Netherlands is attractive to money launderers, particularly through real estate investments. The GON is preparing to exert stricter control on the property sector. A new strategy in 2009 should see tax authorities, financial investigators, and police collaborate more closely on this type of fraud.

The Netherlands has comprehensive anti-money laundering (AML) legislation. The new Prevention of Money Laundering and Financing of Terrorism Act (WWFT) came into force on August 1, 2008. The law incorporates the previous separate acts on identification and reporting (the Services Identification Act and the Disclosure Act). The new law institutes a more risk-based approach. Institutions assess the risk associated with certain clients, products, and transactions. Under the new legislation, institutions also are obliged to verify the identity of a transaction's ultimate beneficial owners.

Banks, bureaux de change, casinos, financing companies, commercial dealers of high-value goods, notaries, lawyers, real estate agents/intermediaries, accountants, business economic consultants, independent legal advisers, tax advisors, trust companies, other providers of trust-related services, life insurance companies, securities firms, stock brokers, and credit card companies in the Netherlands are required to report cash transactions over certain thresholds (varying from 2,000 to 25,000 euros or approximately $2,700 to $34,000), as well as any less substantial transaction that appears unusual (applying a broader standard than "suspicious") to the Netherlands' financial intelligence unit (FIU-NL).

A November 2005 National Directive on money laundering crimes mandates a financial investigation in every serious crime case, sets guidelines for determining when to prosecute for money laundering and provides technical explanations of money laundering offenses, case law, and the use of financial intelligence. Revised indicators determine when an unusual transaction report (UTR) must be filed.

The indicators reflect a partial shift from a rule-based to a risk-based system and are aimed at reducing the administrative costs of reporting unusual transactions without limiting the preventive nature of the reporting system. Amendments to the Dutch legislation expand supervision authority and institute punitive damages. The revised legislation, which became effective on May 1, 2006, also incorporates a terrorist financing indicator in the reporting system.

The GON has developed a policy program to combat serious types of crimes—specifically financial-economic crime, cybercrime and organized crime. The financial-economic crime category includes fraud, money laundering and corruption. The GON intends to implement an extensive package of measures to reinforce existing procedures to combat all aspects of financial crime.

Financial institutions are required by law to maintain records necessary to reconstruct financial transactions for five years after termination of the relationship. There are no secrecy laws or fiscal regulations that prohibit Dutch banks from disclosing client and owner information to bank supervisors, law enforcement officials, or tax authorities. All institutions subject to the reporting and identification requirements, and their employees, are specifically protected by law from criminal or civil liability related to cooperation with law enforcement or bank supervisory authorities. The Money Transfer and Exchange Offices Act, passed in June 2001, requires money transfer offices, as well as exchange offices, to obtain a permit to operate, and subjects them to supervision by the Central Bank. Every money transfer client must be identified and all transactions totaling more than 2,000 euros (approximately $2,700) must be reported to FIU-NL. Sharing of information by Dutch supervisors does not require formal agreements or memoranda of understanding (MOUs).

The FIU-NL is a hybrid administrative-law enforcement unit that in 2006 combined the original administrative FIU, Meldpunt Ongebruikelijke Transacties, or Office for the Disclosure of Unusual Transactions (MOT), with its police counterpart, the Office of Operational Support of the National Public Prosecutor (BLOM). When MOT and BLOM merged, the resulting entity was integrated within the National Police (KLPD). The FIU-NL not only provides an administrative function that receives, analyzes, and disseminates the UTRs and currency transaction reports filed by banks, financial institutions and other reporting entities; it also provides a police function that serves as a point of contact for law enforcement. It forwards suspicious transaction reports (STRs) with preliminary investigative information to the Police Investigation Service.

Obliged entities that fail to file reports with FIU-NL can be sanctioned in two ways. One of the four supervisory bodies, depending on the entity, may impose an administrative fine of up to 32,670 euros (approximately $44,100), depending on the size of the entity. The Dutch Tax Administration supervises commercial dealers; the Bureau Financieel Toezicht or Office for Financial Oversight (BFT) supervises notaries, lawyers, real estate agents, and accountants; the Dutch Central Bank supervises trust companies, casinos, banks, bureaux de change, and insurance companies; and the Authority for Financial Markets supervises clearinghouses, brokers, and securities firms. The public prosecutor may fine nonreporting entities 11,250 euros (approximately $15,200), or penalize individuals failing to report with prison terms of up to two years. Under the Services Identification Act, now incorporated in the WWFT, those subject to reporting obligations must identify their clients, including the identity of beneficial owners, either at the time of the transaction or prior to the transaction, before providing financial services.

Virtually every UTR that is registered by FIU-NL is received electronically through its secure website. The total number of suspicious transactions increased 32 percent from 2006 to 2007. According to FIU-NL, the number of transactions possibly involving terrorist financing doubled from 2006 to 2007. In 2006, FIU-NL received 172,865 UTRs and forwarded 34,531 STRs to the criminal investigative services, totaling over 0.9 billion euros (approximately $1,215,000,000). In 2007, FIU-NL received 214,040 UTRs and forwarded 45,656 STRs. In 2007, the STRs totaled approximately 1.1 billion euros (approximately $ 1,480,000,000). The average amount per suspicious transaction dropped from 26,870

euros (approximately $36,275) in 2006 to 24,000 euros (approximately $32,400) in 2007. This decrease was a direct result of greater use of subjective indicators by reporting institutions. Unusual transaction reports filed on the basis of subjective indicators usually involve smaller amounts than reports filed on the basis of objective indicators. In 2006, 89 percent of UTRs were in euros, eight percent in other European currencies, and three percent involved U.S. dollars.

The number of reports related to money transfers increased in 2007 for the third consecutive year. Money transfer bureaus account for 90 percent of the total volume of suspicious transactions, but only nine percent of the value. The largest number of outgoing suspicious money flows went to Suriname (5,368 money transfers). The greatest total value of suspicious money transfers went to Turkey, over 9 million euros (approximately $12,150,000).

It is noteworthy that most incoming money transfers to the Netherlands are in amounts greater than 2,000 euros (approximately $2,700) except for the money transfers from the United States. Seventy percent of unusual reports of money transfers originating from the United States are lower than the 2,000 euro (approximately $2,700) reporting threshold.

The retention period for suspicious transactions is ten years. To facilitate the forwarding of STRs, FIU-NL has an electronic network called Intranet Suspicious Transactions (IST). Fully automated matches of data from the police databases are included with the UTR data forwarded to enforcement agencies. On January 1, 2003, the former MOT and BLOM organizations together created a special unit (the MBA unit) to analyze data generated from the IST. Under the new FIU-NL structure, the MBA continues to analyze IST data and forwards reports to the police. Since the money laundering detection system also covers areas outside the financial sector, the system is used for detecting and tracing terrorist financing activity. FIU-NL provides the AML division of Europol with STRs, and Europol applies the same analysis tools as the FIU.

In 2007, the notary sector supervisor, BFT, reported that seven notaries allegedly violated AML rules, but due to client confidentiality, the names of the notary firms were not released. Reportedly, the firms facilitated quick transfers of property ownership and received cash payments above the reporting threshold and failed to report. BFT investigators found 124 suspicious cases in 2007 where notaries refused to disclose transactions, and 192 such cases in 2006. In the face of mounting criticism, notary firms are becoming more willing to reveal privileged attorney-client information.

In June 2007, the Netherlands implemented EU regulation 1889/2005 which requires natural persons to declare when they enter or depart the EU carrying 10,000 euros (approximately $13,500) or more in cash. The declarations must be made to Customs. The Dutch Tax and Customs Administration makes all these declarations available to FIU-NL. In 2007, 77 percent of the 770 reported declarations concerned the import of cash and 23 percent the export of cash. Fifty-nine percent of import declarations involved euros and 31 percent U.S. dollars. Fifty-seven percent of export declarations involved euros and 37 percent U.S. dollars. Other declarations involved 32 different currencies.

The Dutch use specially trained dogs at ports and airports to identify cash smugglers. In 2006, these trained dogs found four million euros (approximately $5,400,000) in passenger luggage at Schiphol airport. In February 2008, Dutch authorities arrested three people at Schiphol airport as they attempted to smuggle 630,000 euros (approximately $850,500) out of the Netherlands. In 2008, the Fiscal Information and Investigation Service—Economic Investigation Service (FIOD-ECD) directed operations against trade-based schemes. U.S. law enforcement agencies in the Netherlands have coordinated with Dutch authorities on a trade-based fraud case.

In 2006, the Public Prosecution Office served a summons to suspects of money laundering offenses in 593 cases. Three hundred sixty-nine cases resulted in money-laundering convictions, 36 cases resulted in acquittals, 68 cases were settled with the Public Prosecution Office, 92 cases were dismissed and the others are still pending in court. In 2007, the Public Prosecution Office served a summons to

suspects of money laundering offenses in 756 cases. One hundred ninety-six cases resulted in money-laundering convictions, 17 cases resulted in acquittals, 15 cases were settled with the Public Prosecution Office, 70 cases were dismissed and over 400 are still pending in court.

The Netherlands Court of Audit reported in June 2008 that 63 percent of money laundering cases referred to the Office of Public Prosecution resulted in a conviction. One money laundering acquittal in 2008 drew particular attention. In March, an appeals court overturned the 2006 convictions of the former chief executive officer and chief financial officer of bankrupt airline Air Holland. The two had been accused of laundering proceeds from cocaine sales.

The Netherlands has enacted legislation governing asset forfeiture. The 1992 Asset Seizure and Confiscation Act enables authorities to confiscate assets that are illicitly obtained or otherwise connected to criminal acts. The GON amended the legislation in 2003 to improve and strengthen the options for identifying, freezing, and seizing criminal assets. The police and several special investigation services are responsible for enforcement in this area. These entities have adequate powers and resources to trace and seize assets. All law enforcement investigations into serious crime may integrate asset seizure.

Authorities may seize any tangible assets, such as real estate or other conveyances that were purchased directly with proceeds tracked to illegal activities. Both moveable property and claims are subject to confiscation. Assets can be seized as a value-based confiscation. Legislation defines property for the purpose of confiscation as "any object and any property right" and provides for the seizure of additional assets controlled by a drug-trafficker. Proceeds from narcotics asset seizures and forfeitures are deposited in the general fund of the Ministry of Finance.

To facilitate the confiscation of criminal assets, the GON has instituted special court procedures that enable law enforcement to continue financial investigations to prepare confiscation orders after the underlying crimes have been successfully adjudicated. All police and investigative services in the field of organized crime rely on the real time assistance of financial detectives and accountants, as well as on the assistance of the Proceeds of Crime Office (BOOM), a special bureau advising the Office of the Public Prosecutor in international and complex seizure and confiscation cases. The regular Public Prosecutor's offices are in charge of cases in which under 100,000 euros (approximately $135,000) in assets are seized; BOOM is in charge of cases in which over 100,000 euros (approximately $135,000) in assets are seized. To further international cooperation in this area, BOOM played a leading role in the creation of an informal international network of asset recovery specialists aiming to exchange information and share expertise. Known as the Camden Asset Recovery Network (CARIN), this network was established in The Hague in September 2004.

Statistics provided by the Office of the Public Prosecutor show that the assets seized in 2007 amounted to 23.6 million euros (approximately $31,860,000). Although the total amount remained low, this was a substantial increase over the 17.0 million euros (approximately $22,950,000) seized in 2006 and 17.5 million euros (approximately $23,625,000) in 2005. The United States and the GON have had an asset-sharing agreement in place since 1994. The Netherlands also has an asset-sharing treaty with the United Kingdom, and an agreement with Luxembourg.

In practice, Dutch public prosecutors move to seize assets in only a small proportion of money laundering cases. This is due to a shortage of trained financial investigators and a compartmentalized approach where the financial analysts and operational drug investigation teams often do not act in unison. Increasing seizures of criminal assets is a priority. In 2009, the GON will submit new legislation to make asset forfeiture more robust. The aim is to strengthen the authorities' ability to seize assets after a confiscation measure has been imposed in a case. The police and Public Prosecutor will be allowed to use broader investigative techniques with a court's consent. The GON also intends to take additional measures to make asset forfeiture more efficient. Competent authorities will receive more powers and resources. BOOM is already expanding. In the near future BOOM will also function

as the point of contact for international cases concerning confiscation and seizure, thereby enhancing the sharing of information and best practices.

Terrorist financing is a crime in the Netherlands. In August 2004, the Act on Terrorist Crimes became effective. The Act makes conspiracy to commit a terrorist act a criminal offense. In 2004, the government created a National Counterterrorism Coordinator's Office to streamline and enhance Dutch counterterrorism efforts.

UN resolutions and EU regulations form a direct part of the national legislation on sanctions in the Netherlands. The 1977 "Sanction Provision for the Duty to Report on Terrorism," (Sanctions Law 1977) was amended in June 2002 to implement European Union (EU) Regulation 2580/2001. UNSCR 1373 is implemented through Council Regulation 2580/01; listing is through the EU-wide 931Working Party that replaced the previous informal EU "clearinghouse" with more formal mechanisms. The Netherlands does not require a collective EU decision to identify, freeze, and seize assets suspected of being linked to terrorism nationally. In these cases, the Minister of Foreign Affairs and the Minister of Finance make the decision to execute the asset freeze. Decisions take place within three days after a target is identified. Authorities have used this instrument several times in recent years. In three cases, national action followed as soon as possible after action on the EU level. In one case, the entity was included in the UN 1267 list and thus included in the EU list; in two others, the Netherlands successfully nominated the entity/individual for inclusion in the autonomous EU list.

The ministerial decree that provides authority to the Netherlands to identify, freeze, and seize terrorist finance assets also requires financial institutions to report to FIU-NL all attempted or completed transactions involving persons, groups, and entities that have been linked, either domestically or internationally, with terrorism. Any terrorist crime automatically qualifies as a predicate offense under the Netherlands "all offenses" regime for predicate offenses of money laundering. Involvement in financial transactions with suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list or designated by the EU has been made a criminal offense. UNSCR 1267/1390 is implemented through Council Regulation 881/02. In the Netherlands, Sanctions Law 1977 also addresses this requirement parallel to the regulation.

The 2004 Act on Terrorist Offenses introduces Article 140A of the Criminal Code, which criminalizes participation in a terrorist organization, and defines participation as membership or providing provision of monetary or other material support. Article 140A carries a maximum penalty of fifteen years' imprisonment for participation in, and life imprisonment for leadership of, a terrorist organization. Nine individuals were convicted in March 2006 on charges of membership in a terrorist organization. Legislation expanding the use of special investigative techniques was enacted in February 2007.

UTRs filed by the financial sector act as the first step against the abuse of religious organizations, foundations and charitable institutions for terrorist financing. No individual or legal entity using the financial system (including churches and other religious institutions) is exempt from the client identification requirement. Financial institutions also must inquire about the identity of the ultimate beneficial owners. The second step, provided by Dutch civil law, requires registration of all active foundations with the Chambers of Commerce. Each foundation's formal statutes (creation of the foundation must be certified by a notary of law) must be submitted to the Chambers. Charitable institutions also register with, and report to, the tax authorities to qualify for favorable tax treatment. Approximately 15,000 organizations (and their managements) are registered in this way. The organizations must file their statutes, showing their purpose and mode of operation, and submit annual reports. Samples are taken for auditing. Finally, many Dutch charities are registered with or monitored by private "watchdog" organizations or self-regulatory bodies, the most important of which is the Central Bureau for Fund Raising. In April 2005, the GON approved a plan to improve Dutch efforts to fight fraud, money laundering, and terrorist financing by replacing the current initial screening of

founders of private and public-limited partnerships and foundations with an ongoing screening system. Following a series of legal and technical delays, the GON will introduce the new system in January 2010.

Certain groups of immigrants use informal banks to send money to their relatives in their countries of origin. Indicators point to the misuse of these informal banks for criminal purposes, including a small number of informal bankers deliberately engaging in money laundering transactions and cross-border transfers of criminal money. Initial research by the Dutch police and FIOD/ECD indicates the number of informal banks and hawaladars in the Netherlands is rising. The GON has implemented improved procedures for tracing and prosecuting unlicensed informal or hawala-type activity, with the Dutch Central Bank, FIOD/ECD, the interagency Financial Expertise Center, and the Police playing coordinating and central roles. Approximately 20 to 30 hawaladars are registered in the Netherlands as money service bureaus. Despite these efforts to constrict illegal hawala activity, Dutch officials estimate that substantial sums of money still flow through illegal operations. In Amsterdam, a special police unit investigates underground banks. These investigations have resulted in the disruption of several large money laundering operations.

The United States enjoys strong cooperation with the Netherlands in fighting international crime, including money laundering. A mutual legal assistance treaty (MLAT) between the Netherlands and the United States has been in force since 1983. The Netherlands also has ratified the bilateral implementing instruments for the U.S.-EU MLAT and extradition treaties. The U.S.-EU MLAT is expected to come into force in 2009. One provision included in the U.S.-EU legal assistance agreement will facilitate the exchange of information on bank accounts. The Dutch Ministry of Justice and the Dutch National Police work together with U.S. law enforcement authorities in the Netherlands on operational money laundering initiatives. Although U.S. requests for operational assistance via the mutual legal assistance treaty often are not approved in a timely manner, Dutch officials indicate their Justice Ministry may be able to "streamline" certain aspects of the approval process.

The GON is a member of the Financial Action Task Force (FATF) and the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), a FATF-style regional body (FSRB). The Netherlands was a founding member of the CARIN asset-recovery network, and participates in the Caribbean Financial Action Task Force, a FSRB, as a Cooperating and Supporting Nation. The FIU-NL is a member of the Egmont Group. The Netherlands is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Corruption, and the UN Convention against Transnational Organized Crime.

The Government of the Netherlands should continue its shift to the risk-based approach throughout its regulatory and anti-money laundering/counterterrorist financing (AML/CTF) regime. The GON should devote more resources toward getting better data and a better understanding of alternative remittance systems in the Netherlands, and channel more investigative resources toward tracing these systems. The GON should focus on confiscation of criminal assets, stronger supervision of notaries and other nonbank facilitators of money laundering, and better coordination across ministries. The Netherlands should take steps to increase the expertise within its enforcement authorities to handle more serious and complex cases. Additionally, the GON should continue its active participation in international AML/CTF fora and its assistance to jurisdictions with nascent or developing AML/CTF regimes.

Netherlands Antilles

The Netherlands Antilles is considered a regional financial center and a transshipment point for drugs from South America bound for the United States and Europe. The Netherlands Antilles is comprised of the islands of Curacao, Bonaire, Dutch Saint Maarten, Saba, and Saint Eustatius. Though a part of

the Kingdom of the Netherlands, the Netherlands Antilles has semi- autonomous control over its internal affairs. The Kingdom retains authority over defense, foreign affairs, final judicial review, human rights and good governance. The Government of the Netherlands Antilles (GONA) is located in Willemstad, the capital of Curacao, which is also the financial center for the five islands. Money laundering is primarily related to proceeds from illegal narcotics. Money laundering organizations can take advantage of banking secrecy and use off-shore banking and incorporation systems, economic zone areas, and resort/casino complexes to place, layer and launder drug proceeds. The GONA Ministry of Finance is considering the feasibility of developing an Islamic finance sector in an effort to remain a top international financial center. A significant offshore sector and loosely regulated free trade zones, as well as narcotics trafficking and a lack of border control between Saint Maarten (the Dutch side of the island) and St. Martin (the French side), create opportunities for money launderers in the Netherlands Antilles.

The Netherlands Antilles' banking sector consists of seven local general banks, 14 investment institutions, one subsidiary of a foreign general bank, two branches of foreign general banks, 12 credit unions, six specialized credit unions, one savings bank, four savings and credit funds, 15 consolidated international banks, 18 nonconsolidated international banks, and 22 pension funds. The laws and regulations on bank supervision provide that international banks must have a physical presence and maintain records on the island. There are multiple insurance companies, including three subsidiaries of foreign life insurance companies, seven branches of foreign life insurance companies, six subsidiaries of foreign nonlife insurance companies, six branches of foreign insurance companies, and six independent insurance companies. In addition, there are two captive life insurance companies, 13 captive nonlife insurance companies, and four professional reinsurance companies.

The Netherlands Antilles has an offshore financial sector with 84 trust service companies providing financial and administrative services to an international clientele, which includes offshore companies, mutual funds, and international finance companies. As of September 2007, there were a total of 14,191 offshore companies registered with the Chamber of Commerce in the Netherlands Antilles, as is required by law. International corporations may be registered using bearer shares. The practice of the financial sector in the Netherlands Antilles is for either the bank or the company service providers to maintain copies of bearer share certificates for international corporations, which include information on the beneficial owner(s). The Netherlands Antilles also permits Internet gaming companies to be licensed on the islands. There are currently four-operator member and nine non-operator member licensed Internet gaming companies.

Money laundering is a criminal offense in the Netherlands Antilles under the 1993 National Ordinance on the penalization of money laundering (O.G. 1993, no. 52), as amended by a 2001 National Ordinance (O.G. 2001, no. 77). This legislation establishes that prosecutors do not need to prove that a suspected money launderer also committed an underlying crime to obtain a money laundering conviction. Structuring or "smurfing" is a relatively common occurrence in the Netherlands Antilles, but does not represent high-level money laundering activity, which is accomplished almost exclusively through wire transfers between the Netherlands and the Netherlands Antilles.

The Central Bank of the Netherlands Antilles supervises all banking and credit institutions, including banks for local and international business, specialized credit institutions, savings banks, credit unions, credit funds, and pension funds. The Central Bank also supervises insurance companies, insurance brokers, mutual funds and administrators of these funds, and company service providers, all of which must be licensed by the Central Bank. The Central Bank has issued anti-money laundering guidelines for banks, insurance companies, pension funds, money transfer services, financial administrators, and company service providers. The guidelines also specifically include terrorist financing indicators. Entities under supervision must submit an annual statement of compliance. The Central Bank has provided training to different sectors on the guidelines and established the Financial Integrity Unit to monitor corporate governance and market behavior.

Both bank and nonbank financial institutions, such as company service providers and insurance companies, are required by law to report suspicious transactions to the financial intelligence unit (FIU), the Meldpunt Ongebruikelijke Transacties (MOTNA) established under the Ministry of Finance in 1997 pursuant to Article 2 of the National Ordinance Reporting Unusual Transactions. Obligated entities are also required to report all transactions over NAF 250,000 (approximately $142,000). Banks are required to maintain records for ten years and all other financial intermediaries must maintain records for five years. The GONA is currently amending its legislation to add designated nonfinancial businesses and professions as reporting entities, including lawyers, accountants, notaries, jewelers and real estate agents. It is expected the legislation will be passed in 2009, and MOT NA will be designated as the Supervisory Authority for this sector.

The National Ordinance Obligation to Report Cross-Frontier Money Transportations requires, as of May 2002, everyone entering or leaving one of the island territories of the Netherlands Antilles to report the transport of NAF 20,000 (approximately $11,300) or more, in cash or bearer instruments to Customs officials. This provision also applies to those entering or leaving who are demonstrably traveling together and who jointly carry with them money exceeding NAF 20,000. The declaration must include origin and destination. Violators may be fined up to NAF 250,000 (approximately $142,000) and/or face one year in prison. All cash declaration and smuggling reports are entered into the customs' database and are sent to the financial intelligence unit (FIU) and entered into its database.

In February 2001, the GONA approved proposed amendments to the free zone law to allow e-commerce activities into these areas (National Ordinance Economic Zone no.18, 2001) and renamed these areas Economic Zones (e-zones.) It is no longer necessary for goods to be physically present within the zone. Seven areas within the Netherlands Antilles qualify as e-zones, five of which are designated for e-commerce. The remaining two e-zones, located at the Curacao airport and harbor, are designated for goods. Trade based money laundering from one of two e-zones in the Netherlands Antilles is a well known and preferred method of laundering in the region. Bulk cash smuggling is a continuing problem due to the close proximity of the Netherlands Antilles to Venezuela and Colombia. There have been limited seizures of several thousand dollar increments throughout the past year which intelligence reflects were en route to South America or inbound to one of the e-zone facilities. Law enforcement intervention is very difficult due to host nation laws that apply to the e-zones and tend to exclude law enforcement efforts inside the zone. "Know your customer" practices, while widely publicized by law enforcement, are not required by any statue or rule of business. In many cases, establishing a front company to carry out these endeavors is practiced. These zones are minimally regulated; however, administrators and businesses in the zones have indicated an interest in receiving guidance on detecting unusual transactions. There is not a significant black market for smuggled goods.

In 2000, the GONA enacted the National Ordinance on Freezing, Seizing and Forfeiture of Assets Derived from Crime. The law allows the prosecutor to seize the proceeds of any crime proven in court. Civil forfeiture is not permitted. The GONA enacted legislation in 2002 allowing a judge or prosecutor to freeze assets related to the Taliban and Usama Bin Laden, as well as all persons and companies connected with them. The legislation contains a list of individuals and organizations suspected of terrorism. The Central Bank instructed financial institutions to query their databases for information on the suspects and to immediately freeze any assets found. In October 2002, the Central Bank instructed the financial institutions under its supervision to continue these efforts and to consult the UN website for updates to the list.

In 2008, the GONA issued the National Ordinance on the Penalization of Terrorism, Terrorism Financing and Money Laundering (O.G. 2008, no. 46) which became effective as of June 2008. A financial institution that carries out a transaction, knowing that the funds or property involved are owned or controlled by terrorist or terrorist organizations, or that the transaction is linked to, or likely to be used in, terrorist activity, is committing a criminal offense. Such an offense may exist regardless

of whether the assets involved in the transaction were the proceeds of criminal activity or were derived from lawful activity but intended for use in support of terrorism. In June 2008, the GONA approved an amendment to the Penal Code to cover terrorism and the funding of terrorist activities related to money laundering. The penalty is four to 20 years imprisonment and a maximum fine of $600,000.

MOT NA is an administrative FIU with no criminal investigative responsibilities. The FIU collects and analyzes data, has access to all records and databases of all governmental entities with law enforcement powers, refers all transactions suspected of being related to money laundering and/or terrorist financing to the Central Police and Prosecutor, prepares reports on money laundering trends and renders annual reports and strategies to the Ministers of Finance and Justice. MOT NA annually receives approximately between 11,000-12,000 suspicious transaction reports (statistics for 2008 were not available). The MOT NA currently has a staff of nine, and is engaged in increasing the effectiveness and efficiency of its reporting system. Progress has been reported in automating suspicious activity reporting. Additionally, the MOT NA has issued a manual for casinos on how to file reports and has started to install software in casinos that will allow reports to be submitted electronically. The Government of the Netherlands plans to provide technical support to the MOT NA to improve their analytical capabilities with regard to terrorist financing.

Netherlands Antilles' law allows the exchange of information between the MOT NA and foreign FIUs by means of memoranda of understanding (MOU) and by treaty. The MOT NA's policy is to answer requests within 48 hours of receipt. A tax information exchange agreement (TIEA) between the Kingdom of the Netherlands (KON) and the United States with regard to the Netherlands Antilles, signed in 2002, entered into force in March 2007. The Mutual Legal Assistance Treaty between the KON and the United States applies to the Netherlands Antilles; however, the treaty is not applicable to requests for assistance relating to fiscal offenses addressed to the Netherlands Antilles. The U.S.-KON Agreement Regarding Mutual Cooperation in the Tracing, Freezing, Seizure and Forfeiture of Proceeds and Instrumentalities of Crime and the Sharing of Forfeited Assets also applies to the Netherlands Antilles.

The MOT NA is a member of the Egmont Group. The Netherlands Antilles is a member of the Caribbean Financial Action Task Force (CFATF), and as part of the Kingdom of the Netherlands, participates in the Financial Action Task Force (FATF). In November 2009, the Netherlands Antilles will assume the chair of CFATF. The Netherlands Antilles is also a member of the Offshore Group of Banking Supervisors. The Kingdom of the Netherlands has extended its ratification of the 1988 UN Drug Convention to the Netherlands Antilles. The Kingdom of the Netherlands became a party to the UN International Convention for the Suppression of the Financing of Terrorism in 2002. In accordance with Netherlands Antilles' law, which stipulates that all the legislation must be in place prior to ratification, the GONA is preparing legislation to enable the Netherlands to extend ratification of the Convention to the Netherlands Antilles. Likewise, the Kingdom of the Netherlands has not yet extended ratification of the UN Convention against Transnational Organized Crime or the UN Convention against Corruption to the Netherlands Antilles.

The Government of the Netherlands Antilles has demonstrated a commitment to combating money laundering. The Netherlands Antilles should continue its focus on increasing regulation and supervision of the offshore sector and free trade zones, as well as pursuing money laundering investigations and prosecutions. The GONA should ensure that anti-money laundering regulations and reporting requirements are extended to designated nonfinancial businesses and professions. The Netherlands Antilles should work to fully develop its capacity to investigate and prosecute money laundering and terrorist financing cases.

Nicaragua

Nicaragua is not a regional financial center or a major drug producing country. However, it continues to serve as a significant transshipment point for South American cocaine and heroin destined for the United States and Europe. There is evidence that the narcotics trade is increasingly linked to arms trafficking. This situation, combined with weak rule of law, judicial corruption, the politicization of the public prosecutor's office and the Supreme Court, as well as insufficient funding for law enforcement institutions, makes Nicaragua's financial system an attractive jurisdiction for money laundering. Nicaragua's location—with access to both the Atlantic and the Pacific Oceans, porous border crossings to its north (Honduras) and south (Costa Rica), and a sparsely inhabited and underdeveloped Atlantic Coast area—makes it an area heavily used by transnational organized crime groups, including human and drug trafficking organizations. These groups also benefit from Nicaragua's weak legal system and its ineffective fight against financial crimes, money laundering, human trafficking, and the financing of terrorism. Nicaraguan officials have expressed concern that, as neighboring countries have tightened their anti-money laundering laws, established financial intelligence units (FIUs), and taken other enforcement actions, more illicit money has moved into the vulnerable Nicaraguan financial system. Additionally, the continued politicization of the Nicaraguan judicial system and the willingness of the current administration to use the financial regulatory system as a tool to attack political adversaries seriously undermine the integrity of the anti-money laundering and overall law-enforcement regimes in Nicaragua.

The Government of Nicaragua (GON) does not permit direct offshore banking operations, but it does permit such operations through nationally chartered entities. Bank and company bearer shares are permitted. Nicaragua has a substantial gambling industry that remains largely unregulated. Two competing casino regulation bills are currently in the National Assembly; the main difference between the bills is whether the existing tax authority will have regulatory power or whether an independent institution will be established for that purpose. The Nicaraguan government has shown little interest in either of these bills, both of which are languishing in the National Assembly. The tax authority, however, has successfully implemented regulations to tax the casino industry. There are no Internet gaming sites in Nicaragua.

There is a sizeable international component to Nicaragua's financial sector. A number of foreign institutions have recently bought significant shares of Nicaraguan financial institutions, including GE Consumer Finance and HSBC, which purchased Banistmo, a Panamanian bank, and now operates as HSBC in Nicaragua. Most large Nicaraguan banks already maintain correspondence relationships with Panamanian institutions. In 2008, Citibank finalized the purchase of Banco Uno, a retail bank with a large consumer credit unit. The recent completion of several Free Trade Agreements (FTAs)—including the Central America-Dominican Republic-United States FTA (CAFTA-DR), as well as bilateral FTAs with Taiwan, Mexico, the Dominican Republic, and Panama—also suggests growing involvement of Nicaraguan financial institutions with international partners and clients.

As of February 2008, a total of 121 companies operated in 32 designated free trade zones (FTZs), or "industrial parks" as they are called in Nicaragua, employing 89,000 workers and generating exports of $1.1 billion. The National Free Trade Zone Commission (CNZF), a government agency, regulates all FTZs and the companies located in them. The Nicaraguan Customs Agency also monitors all FTZ imports and exports. Reportedly, while there is no indication that these FTZs are being used in trade-based money laundering schemes or by the financiers of terrorism, a June 2007 inspection by U.S. Customs agents uncovered evidence of transshipments of Chinese-made apparel.

A new criminal code came into force in June 2008; this new code aims to bring Nicaragua's anti-money laundering and counterterrorist financing regime into greater compliance with international standards set by the Financial Action Task Force (FATF). The new code criminalizes terrorist financing, bulk cash smuggling, and money laundering beyond drug-related offenses; expands legal

protection for the financial sector; and defines crimes against the banking and financial system. While passage of the new criminal code is a positive move forward for the GON, it will likely take a longer period of time before all aspects of the penal code are implemented in a uniform manner in the Nicaraguan justice system. Further, the new code reduces the penalty for money laundering to a recommended maximum sentence of five years.

While adoption of the new criminal code demonstrates a commitment to thwart the financing of terrorism, money laundering, and other financial crimes, other factors—including limited resources, corruption (including in the judiciary), and the lack of political will in some sectors continue to complicate efforts to counteract these criminal activities. Nicaragua's lack of an FIU also fundamentally limits the extent to which the GON can effectively combat money laundering and other financial crimes. However, in 2008, the GON investigated four money laundering cases—three through the Attorney General's Office and one through the Office of the Prosecutor General. Also, in 2008 the National Prosecutor's Office prosecuted three cases of cash smuggling involving a total of $195,610.

Law 285 (posted in 1999) requires all financial institutions under the supervision of the Superintendent of Banks and Other Financial Institutions (SIBOIF), including stock exchanges and insurance companies, to report cash deposits over $10,000 and suspicious transactions to the SIBOIF and to keep records for five years. The SIBOIF then forwards reports to the Commission of Financial Analysis (CAF). All financial institutions not supervised by SIBOIF, including attorneys, notaries, accountants, and real estate agents, are required to report suspicious transactions directly to the CAF. All persons entering or leaving Nicaragua are also required to declare the transportation of currency in excess of $10,000 or its equivalent in foreign currency. However, cash smuggling is only considered a customs violation under Nicaraguan law. Bank officials are held responsible for all of their institution's actions, including failure to report money laundering, and sanctions may be imposed on financial institutions and professionals of the financial sector, including internal auditors, who do not develop anti-money laundering programs or do not report to the appropriate authorities suspicious and unusual transactions that may be linked to money laundering, as required by the anti-money laundering law.

The SIBOIF is considered to be an independent and reputable financial institution regulator. The position of the Superintendent does not enjoy legal immunity, exposing the Superintendent to lawsuits from regulated institutions. Similarly, officers in financial institutions charged with reporting suspicious transactions to the SIBOIF are not legally protected with regard to their cooperation. Given the corruption in the judicial system, this exposure can limit the willingness of SIBOIF to make "unpopular" decisions; however, the institution's financial experts have reached out to the Nicaraguan National Police (NNP) to work with them. The SIBOIF has regularly fined banks for not reporting suspicious transactions. The willingness of the SIBOIF and NNP to investigate financial crimes, and a substantial level of cooperation between the Attorney General's Office and the NNP on financial crimes and money laundering issues, has resulted in greater adherence by banks to the reporting requirements contained in Law 285.

On paper, the CAF is comprised of representatives from various elements of law enforcement and banking regulators and is responsible for detecting money laundering trends, coordinating with other agencies and reporting its findings to Nicaragua's National Anti-Drug Council. But the CAF does not analyze the information received, and is not considered to be a professional or independent unit. It is ineffective due to an insufficient budget, the politicization of its leadership, and a lack of fully dedicated, trained personnel, equipment and strategic goals. All of its members have primary responsibilities at their parent institutions, which take precedence over CAF duties. The CAF is headed by the National Prosecutor, who receives the reports from banks and decides whether to refer them to the NNP for further investigation. In 2008, the Caribbean Financial Action Task Force (CFATF) visited Nicaragua to assess the GON's anti-money laundering regime, with a specific focus on the activities of the CAF. CFATF is scheduled to release this assessment by summer 2009.

The NNP's Economic Crimes Unit and the Office of the National Prosecutor are in charge of investigating financial crimes, including money laundering and terrorist financing. The Office of the National Prosecutor is in the process of creating its own Economic Crimes Unit to work in tandem with the NNP. The unit has been conducting investigations into money laundering and drug related crimes since March 2007 and has worked closely with the offices of both the Attorney General and the Prosecutor General.

During 2008, Embassy Managua continued to support Nicaraguan National Assembly efforts to enact legislation creating an independent FIU. These efforts included bringing a delegation of Nicaraguan legislators, law enforcement officials, and economic policy experts to participate in anti-money laundering meetings and consultations with regional FIU representatives on the possibility of creating a Nicaraguan FIU. Nicaraguan legislators have expressed a strong and continuing commitment to ensure that the FIU legislation will create an independent unit compliant with Egmont Group standards, with an additional focus on incorporating regulatory safeguards against political tampering with the proposed new unit.

Through five SIBOIF administrative decrees, the GON also has the authority to identify, freeze, and seize terrorist-related assets, but has not yet identified any such active cases. Reportedly, there are no hawala or other similar alternative remittance systems operating in Nicaragua, and the GON has not detected any use of gold, precious metals or charitable organizations to disguise transactions related to terrorist financing. However, there are informal "cash and carry" networks for delivering remittances from abroad that may be indicative of money laundering. The NNP is currently investigating possible instances of money laundering involving cash remittances from Europe.

An emerging issue of concern is the current administration's politically motivated accusations that international and Nicaraguan NGOs, particularly those involved in pro-democracy activities, are complicit in money laundering schemes. Despite the lack of formal criminal charges, the Prosecutor's Office has worked with the NNP to raid and seize the financial records of several pro-democracy and civil society NGOs. Administration officials specifically pointed to the assignment of sub-grants by certain NGOs to other organizations as evidence of possible money laundering activity. Under the current Nicaraguan penal code, however, an activity can only be considered money laundering if the original source of funding is illicit or unknown. As the NGOs in question receive their funding in a transparent manner from donor governments and other established international groups, many observers argue that this attempt to apply money laundering statutes to the groups is an illegitimate application of the law.

There are more than 300 microfinance institutions (MFI) in Nicaragua, serving more than 300,000 clients and handling at least $400 million. MFIs in Nicaragua dominate the informal economy and manage a significant portion of the remittances. Over half of this market is handled by five institutions that have now converted into formal banks. While the five MFIs that are now formal banks are regulated by the SIBOIF, the others are currently unregulated. These institutions are, however, still subject to the reporting requirements in Law 285 and to financial crimes listed in the current criminal code. Any crimes committed fall under the jurisdiction of the NNP's Economic Crimes Unit and the National Prosecutor's Office.

Nicaragua is a party to the 1988 UN Drug Convention, the UN International Convention on the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. The GON has also ratified the Inter-American Convention on Mutual Legal Assistance in Criminal Matters and the Inter-American Convention against Terrorism. Nicaragua is a member of the Money Laundering Experts Working Group of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD), and the Caribbean Financial Action Task Force (CFATF). is the only country in Central America, and one of few countries in the Americas, that does not have a functional FIU. Due to continued corruption

in the Nicaraguan judiciary, the United States ceased direct assistance to the Nicaraguan Supreme Court.

The GON has made some progress in its efforts to combat financial crime by expanding the predicate offenses for money laundering beyond narcotics trafficking and criminalizing terrorist financing. The GON should continue recent progress by taking the necessary steps to fully implement the new criminal code. Nicaragua should also redouble its efforts to create an effective FIU; this would enable it to share financial information with other FIUs globally. Nicaragua should also develop a more effective method of cooperating and exchanging information with foreign law enforcement agencies. The GON should take steps to immobilize all bearer shares and prohibit further issuance. The GON would also benefit from concentrating its financial crime investigation efforts on entities and institutions that are known to be involved in criminal behavior, and should halt its political interference in the operations of the financial regulatory and law enforcement agencies, as well as with NGOs for which there is no evidence laundering money. These actions, coupled with increased enforcement of existing legislation and implementing regulations, would significantly strengthen the country's anti-money laundering and counterterrorist financing regime, and could help bring Nicaragua closer to compliance with relevant international anti-money laundering and counterterrorist financing standards and controls.

Nigeria

Nigeria is a major drug trans-shipment point and a significant center for criminal financial activity. Individuals and criminal organizations have taken advantage of the country's location, porous borders, weak laws, systemic corruption, lack of enforcement, and poor socioeconomic conditions to launder the proceeds of crime. Proceeds from drug trafficking, illegal oil bunkering, bribery and embezzlement, contraband smuggling, theft, and financial crimes such as bank fraud, real estate fraud, and identity theft constitute major sources of illicit proceeds in Nigeria. Advance fee fraud, as also known as "419" fraud in reference to the fraud section in Nigeria's criminal code, is a lucrative financial crime that generates hundreds of millions of illicit dollars annually. Money laundering in Nigeria takes many forms, including investment in real estate; wire transfers to offshore banks; political party financing; deposit in foreign bank accounts; use of professional services, such as lawyers, accountants, and investment advisers; and cash smuggling. Nigerian criminal enterprises are adept at devising ways to subvert international and domestic law enforcement efforts and evade detection. Recent dismissal and reassignment of experienced financial crimes law enforcement personnel call into question government commitment to combating financial crime and corruption in Nigeria, which continues to be plagued by these crimes.

In December 2002, Nigeria passed an amendment to the 1995 Money Laundering Act extending the scope of the law to cover proceeds from predicate offenses other than narcotics trafficking. In 2004, the National Assembly repealed the 1995 Money Laundering Act as amended and passed the Money Laundering (Prohibition) Act, which applies to the proceeds of all financial crimes. Nigeria also passed an amendment to the 1991 Banking and Other Financial Institutions (BOFI) Act expanding coverage to stock brokerage firms and foreign currency exchange facilities, giving the Central Bank of Nigeria (CBN) greater power to deny bank licenses, and allowing the CBN to freeze suspicious accounts. A third piece of legislation, the 2004 Economic and Financial Crimes Commission (Establishment) Act, established the Economic and Financial Crimes Commission (EFCC), the body that investigates and prosecutes money laundering and other financial crimes, and coordinates information sharing. Violation of the Act carries a penalty of up to life imprisonment. Amendments to the 2004 EFCC Act gave the EFCC the authority to investigate and prosecute money laundering, expanded the number of EFCC board members, enabled EFCC police members to bear arms, and banned interim court appeals that hinder the trial court process.

Nigeria also employs the 1995 Foreign Exchange (Monetary and Miscellaneous Provisions) Act. This legislation enhanced the CBN's power under the BOFI to deny bank licenses and freeze suspicious accounts. It also strengthened financial institutions by requiring more stringent monitoring of accounts, removing a threshold for suspicious transactions, and lengthening the period for retention of records.

Money laundering controls apply to banks and other financial institutions, including stock brokerages and currency exchange houses, as well as designated nonfinancial businesses and professions (DNFBPs). These institutions include dealers in jewelry, cars and luxury goods, chartered accountants, audit firms, tax consultants, clearing and settlement companies, legal practitioners, hotels, casinos, supermarkets and other businesses that the Federal Ministry of Commerce (FMC) designates as a money laundering risk. Nigeria has no bank secrecy laws that prevent the disclosure of client and ownership information by domestic financial services companies to bank regulatory and law enforcement authorities.

In May 2006, the Financial Action Task Force visited Nigeria to conduct an evaluation of the revisions made to the government's anti-money laundering (AML) regime. The FATF recognized that the Government of Nigeria (GON) had remedied the major deficiencies in its AML regime and removed Nigeria from its noncooperative countries and territories (NCCT) list. In 2008, the Intergovernmental Task Force against Money Laundering in West Africa (GIABA), conducted, discussed and adopted Nigeria's mutual evaluation.

According to the mutual evaluation report (MER), significant legal gaps exist in Nigeria's AML/CTF regime. In addition, Nigerian authorities have not issued clear guidance to financial institutions, resulting in deficiencies related to customer due diligence, beneficial ownership, record keeping, and reporting requirements. The MER also noted that the FIU's powers under the EFCC are ambiguous, and its statistics on suspicious transaction reports (STRs) and currency transaction reports (CTRs) are inconsistent.

The primary institutions dealing with money laundering and financial crimes are the EFCC, the Nigerian Financial Intelligence Unit (NFIU), the Independent Corrupt Practices Commission (ICPC), and Special Control Unit against Money Laundering (SCUML). The NFIU, established in 2005, derives its powers from the Money Laundering (Prohibition) Act of 2004 and the EFCC Act. Housed within the EFCC, it is the central agency for the collection, analysis and dissemination of information on money laundering and terrorist financing. The NFIU is a significant component of the EFCC, complementing the EFCC's directorate of investigations. It does not carry out its own investigations. The Money Laundering (Prohibitions) Act, Section 6, requires STRs to be submitted by financial institutions and designated nonfinancial businesses and professions, and gives the NFIU the authority to receive them. The NFIU also receives reports involving the transfer to or from a foreign country of funds or securities exceeding U.S. $10,000 in value. All financial institutions and designated nonfinancial institutions are required by law to furnish the NFIU with details of these financial transactions.

The NFIU fulfills a crucial role in receiving and analyzing STRs. The NFIU has access to records and databases of all government and financial institutions, and it has entered into memoranda of understandings (MOUs) on information sharing with several other FIUs. The NFIU is a member of the Egmont Group.

Since its inception in April 2004, the EFCC has held the mandate and the capacity to effectively investigate and prosecute financial crimes, including money laundering and terrorist financing. The EFCC also coordinates agencies' efforts in pursuing financial crime investigations. The EFCC has the authority to prevent the use of charitable and nonprofit entities as money laundering vehicles, although it has not reported any cases involving these entities.

The EFCC previously succeeded in investigating and prosecuting financial crime. Its assault on high-level corruption resulted in the agency receiving the support of the international community as well as the ire of corrupt officials. The EFCC has put forth efforts to enact new laws and to conduct a vigorous public enlightenment campaign, resulting in prosecutions for crimes such as bank fraud and counterfeiting. It has recovered or seized assets from people guilty of fraud both inside and outside of Nigeria, including a syndicate that included highly placed government officials who were defrauding the Federal Inland Revenue Service (FIRS). Several influential individuals have been arrested and are currently awaiting trial. EFCC members also embarked upon a campaign to identify and prosecute former government officials. Some EFCC members have been killed for their efforts to expose and enforce the laws against corruption and financial crime.

In its first 5 years of existence, the EFCC successfully prosecuted 121 cases involving advanced fee fraud ("419") scams, seized over $5 billion in cash and property, and repatriated over $4.6 million to U.S. entities. From October 2007 through September 2008, the EFCC reported 3 money laundering convictions, with 9 pending cases against politically exposed persons and other pending cases related to fraud against U.S. entities. It also reported 87 "419" convictions during that period. The EFCC facilitated the return of fraud proceeds totaling $1.6 million by a prominent Nigerian bank to U.S. entities.

However, in 2008, the EFCC faced significant challenges in fulfilling its mandate to fight financial crimes and money laundering. Senior leadership changes (including the heads of both the EFCC and the NFIU) and the reassignment of key personnel have raised serious concerns about the agency's current capacity and direction. Many of the reassigned personnel had spent years developing substantial skills and experience in investigating and prosecuting money laundering and financial crimes. New personnel reportedly have little experience in conducting the type of rigorous investigations required for complex financial crimes. These developments have cast doubt on the Government's commitment to fight financial crime as well as corruption.

In addition to the EFCC, the National Drug Law Enforcement Agency (NDLEA), the ICPC, and the Criminal Investigation Department of the Nigeria Police Force (NPF/CID) have the authority to investigate financial crimes. Many observers, however, believe that the Nigerian Police Force is incapable of handling financial crimes because of corruption and poor institutional capacity.

The Corrupt Practices and Other Related Offences Act established the ICPC in June 2000. The ICPC is primarily charged with receiving and investigating reports of corruption among Nigeria's large government sector work force and prosecuting offenders where necessary. However, according to its chairman, ICPC's focus has been public information campaigns, not investigations and prosecutions. The agency is independent but effectively lacks support from other government structures and is insufficiently funded. ICPC has anticorruption and transparency units (ACTU) in almost every Federal agency to deal with official misconduct and malfeasance by public servants. If an ACTU determines that there has been criminal behavior, it refers the case to ICPC for prosecution. The ACTUs and the ICPC investigators and prosecutors are under-trained and the agency has been increasingly relying on private lawyers to try cases under contract. The ICPC has recorded 15 convictions in the 8 years it has been operating.

Due to Nigeria's primarily cash-based economy, 90 percent of money laundering activity reportedly takes place in the informal sector. The Special Control Unit Against Money Laundering (SCUML), is a special unit in the Ministry of Commerce which monitors, supervises, and regulates the activities of businesses and professions outside of the formal financial sector thought to pose a money laundering risk. Oversight by the Ministry of Commerce, however, has reportedly not been rigorous or effective. Consequently the EFCC decided to fund SCUML and second some of its employees to that agency in an effort to rapidly improve investigative and enforcement capacity. In addition, the EFCC facilitated the inauguration of a Designated Non-Financial Institution (DNFI) Advisory Council which serves as

a formal platform for partnership between SCUML as the regulator and the heads of the DNFI Self Regulatory Organizations (SROs), including some Civil Society Organizations (CSOs). The EFCC and SCUML have collaborated on efforts to strengthen the Chief Compliance Officers Forum, which EFCC/NFIU facilitated.

While the NDLEA has the authority to handle narcotics-related cases, it does not have adequate resources to trace, seize, and freeze assets. Cases of this nature are usually referred to the EFCC. Depending on the nature of the case, the tracing, seizing, and freezing of assets may be executed by the EFCC, NDLEA, NPF, or the ICPC. The proceeds from seizures and forfeitures pass to the federal government, and the GON uses a portion of the recovered sums to provide restitution to the victims of the criminal acts. The banking community cooperates with law enforcement to trace funds and seize or freeze bank accounts.

Section 20 of the 2004 EFCC Act provides for the forfeiture of assets and properties to the federal government after a money laundering conviction. Foreign assets are also subject to forfeiture. The properties subject to forfeiture are set forth in EFCC Act Sections 24-26, and include any real or personal property representing the gross receipts a person obtains directly as a result of the violation of the act, or traceable to such receipts. They also include any property representing the proceeds of an offense under the laws of a foreign country within which the offense or activity would be punishable for more than one year. All means of conveyance, including aircraft, vehicles, or vessels used or intended to be used to transport or facilitate the transportation, sale, receipt, possession or concealment of the economic or financial crimes is likewise subject to forfeiture. Forfeiture is possible only as part of a criminal prosecution. There is no comparable law providing for civil forfeiture independent of a criminal prosecution, but the EFCC has established a committee to draft legislation to address this deficiency.

Nigeria has attempted to criminalize the financing of terrorism through Section 15 of the EFCC Act. The EFCC has authority under the Act to identify, freeze, seize, and forfeit terrorist finance-related assets; however, implementation of the existing framework has revealed some practical challenges. The EFCC Act does not provide a comprehensive framework for criminalizing and pursuing the full range of terrorist financing as defined by international standards. The Act does not criminalize terrorist financing, nor does it reference terrorist financing as a predicate offence for money laundering. A comprehensive bill for the prevention of terrorism is currently before the National Assembly. If passed, it would be Nigeria's first autonomous anti-terrorism law.

The CBN circular (BSD/13/2006) from August 2006 requires all financial institutions to forward STRs where the suspicious and unusual transactions include potential financing of terrorism to the FIU. Nigerian financial institutions periodically receive the UNSCR 1267 Sanctions Committee's consolidated list and have detected one case of terrorist financing within the banking system. Prosecution of that case is currently pending.

Nigeria is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. Nigeria ranked 121 out of 180 countries in Transparency International's 2008 Corruption Perceptions Index, moving up from 147 in 2007.

The United States and Nigeria have a Mutual Legal Assistance Treaty, which entered into force in January 2003. Nigeria has signed memoranda of understanding with Russia, Iran, India, Pakistan and Uganda to facilitate cooperation in the fight against narcotics trafficking and money laundering. Nigeria has also signed bilateral agreements for information exchange relating to money laundering with South Africa, the United Kingdom, and all Commonwealth and Economic Community of West African States (ECOWAS) countries. Nigeria is a member of GIABA, a FATF-style regional body.

The Government of Nigeria (GON) should ensure the autonomy and independence of the EFCC and NFIU from political pressure. In particular, EFCC needs to produce more effective results through prosecutions and enforcement actions in financial crimes and corruption investigations. The GON should also strengthen SCUML's authority to supervise designated nonfinancial businesses and professions. Nigeria should ensure that the Police Force has the capacity to function as an investigative partner in financial crime cases, as well as work to eradicate any corruption that might exist within that and other law enforcement bodies. Nigeria should re-invigorate its anticorruption program and support the EFCC, as well as the ICPC, in their mandates to investigate and prosecute corrupt government officials and individuals. The GON should consider establishing a special court with specific jurisdiction and trained judges to handle financial crimes. Nigeria should enact a law providing for nonconviction-based forfeiture, ensure full implementation of its AML regime, and promote respect for the rule of law. Nigerian authorities should work toward a regime capable of thwarting money laundering and terrorist financing; and work toward full compliance with all relevant international standards, eliminating its remaining AML shortcomings. Authorities should work toward the passage of the comprehensive anti-terrorism bill in the National Assembly. The GON should continue to engage with the FATF, GIABA and other international organizations.

Pakistan

Pakistan is not considered a regional or offshore financial center; however, financial crimes related to narcotics trafficking, terrorism, smuggling, tax evasion, corruption and fraud are significant problems. Pakistan is a major drug-transit country. The abuse of the charitable sector, smuggling, trade-based money laundering, hawala-hundi, and physical cross-border cash transfers are the common methods used to launder money and finance terrorism in Pakistan. Pakistani criminal networks play a central role in the transshipment of narcotics and smuggled goods from Afghanistan to international markets.

Pakistan does not have firm control of its borders with Afghanistan, Iran and China, facilitating the flow of smuggled goods through the Federally Administered Tribal Areas (FATA) and Baluchistan. Some goods such as foodstuffs, electronics, building materials, and other products transiting Pakistan duty-free under the Afghan Transit Trade Agreement are sold illegally in Pakistan. Counterfeit goods generate substantial illicit proceeds that are laundered. Private unregulated charities are also a major source of illicit funds for international terrorist networks. Some madrassas have been used as training grounds for terrorists and for terrorist funding. The lack of control of madrassas, similar to the lack of control of Islamic charities, allows terrorist and jihadist organizations to receive financial support under the guise of support of Islamic education.

Money laundering and terrorist financing are often accomplished in Pakistan via the alternative remittance system called hundi or hawala. This system is also widely used by the Pakistani people for informal banking purposes, although controls have been significantly tightened since 2002. In June 2004, the State Bank of Pakistan (SBP) required all hawala operators ("hawaladars") to register as authorized foreign exchange dealers and to meet minimum capital requirements. Despite the State Bank of Pakistan's efforts, unlicensed hawaladars still operate illegally in parts of the country (particularly Peshawar and Karachi), and authorities have taken little action to identify and enforce the regulations prohibiting nonregistered hawaladars. Most illicit funds are transacted through these unlicensed operators. Fraudulent invoicing is typical in hawala countervaluation schemes. However, legitimate remittances from the roughly five million Pakistani expatriates residing abroad, sent via the hawala system prior to 2001, now flow mostly through the formal banking sector and have increased significantly to $6.45 billion in fiscal years 2007-08. At least four moneychangers, including a CEO of a leading foreign exchange company, were arrested on November 8, 2008 by Pakistan's Federal Investigation Agency (FIA) for smuggling and illegal cross border transfer of foreign exchange. According to FIA sources, a case was registered against the moneychangers under the Foreign

Exchange Regulations Act of 1947, which does not specify severe penalties for such crimes. FIA sources estimate that foreign exchange sent out of the country could be in the millions of dollars.

Pakistan has established a number of Export Processing Zones (EPZs) in all four of the country's provinces. Although no evidence has emerged of EPZs being used in money laundering, inaccurate invoicing is common in the region and could be used by entities operating out of these zones. In 2007, the Directorate General of Customs Intelligence (DGCI) investigated a well-known Pakistani business group involved with trade-based money laundering. The business over-invoiced the value and quantity of the exports of garments and textiles to Dubai and Saudi Arabia. The chairman of the business group and his partners held 49 percent shares in the Dubai-based company that imported many of the goods. The investigation also revealed that the business group used hawala to transfer large amounts of money and value through a prominent foreign exchange company based in Karachi. From 2001-2007, the value of the trade consignments totaled U.S. $330 million. In fiscal year 2007-2008, no cases of trade-based money laundering were reported.

Pakistan became a member of the Asia/Pacific Group on Money Laundering (APG) in 2000, therefore accepting the APG requirement that members develop, pass and implement anti-money laundering and counterterrorist financing legislation and other measures based on accepted international standards. A high-level APG delegation visited Pakistan in early July 2007 to discuss Pakistan's long-delayed passage of comprehensive anti-money legislation. At its July plenary, APG members agreed that unless Pakistan enacts and proclaims into force consolidated AML legislation or issues a Presidential Ordinance prior to December 31, 2007, Pakistan's membership could be suspended. On September 8, 2007 former President Musharraf signed an AML Ordinance to implement the long-awaited AML bill. While creating this ordinance averted suspension of membership in the APG, Pakistan still has considerable work ahead to meet international standards, especially the core Financial Action Task Force (FATF) recommendations related to the criminalization of money laundering and suspicious transaction reporting.

Some of the weaknesses identified in the AML Ordinance include the following: Not all of the FATF designated categories of offenses (e.g., smuggling, racketeering, trafficking in persons, sexual exploitation, arms trafficking, and environmental crime) are covered as predicate offenses. The intent and knowledge requirement required to prove the offense of money laundering is not consistent with the standards set out in the Vienna and Palermo Conventions. Only the concealment of criminal proceeds is an offense, not the transfer of legitimate money to promote criminal activity. The definition of what constitutes a suspicious transaction is not adequate as it does not cover cases where an individual "suspects" or "has reason to suspect" that funds are the proceeds of criminal activity. The Ordinance also does not contain any specific requirement to report transactions in relation to terrorist financing. The forfeiture procedures set forth in the law are cumbersome and will inhibit the successful seizure and confiscation of property involved in offenses. Additionally, the reporting structure of the Financial Monitoring Unit may affect its independence and effectiveness.

The AML Ordinance established a National Executive Committee (NEC), which is charged with coordinating Pakistan's AML/CTF efforts. The NEC is made up of representatives from the Ministries of Finance, Interior, Foreign Affairs, and Law as well as the SBP, the Securities and Exchange Commission of Pakistan (SECP), and the Financial Monitoring Unit. The NEC established a sub committee to review and recommend changes to the AML Ordinance. In anticipation of an APG mutual evaluation scheduled for early 2009, the GOP has reportedly revised the AML Ordinance to bring it into compliance with the FATF standards. The Cabinet has approved the revised ordinance and the GOP now plans to present it to the Parliament for approval; however the text of the Ordinance has not been made public.

In 2008 the FATF issued two statements concerning Pakistan's AML/CTFregime. On February 28, 2008 the FATF acknowledged Pakistan's progress in adopting AML legislation but advised financial

institutions to be aware of the remaining deficiencies in Pakistan's AML/CTF system, which constitute vulnerability in the international financial system. On October 16, 2008, the FATF issued a second statement reaffirming its position.

The AML Ordinance formally established a Financial Monitoring Unit (FMU) as Pakistan's financial intelligence unit (FIU), within the SBP to receive, analyze, and disseminate suspicious transaction reports. However, it is subject to the supervision and control of the General Committee, comprised of several Government of Pakistan (GOP) cabinet secretaries, thus limiting its independence. Because Pakistan lacks a central repository for the reporting of suspicious transaction reports and the absence of provisions to protect institutions from liability for reporting, very few suspicious transactions have been reported or analyzed. From July 2007 through June2008, 130 suspicious transactions were reported to the State Bank by various banks and seven were referred to law enforcement agencies for investigation. The FMU has 15 staff members.

Several law enforcement agencies are responsible for enforcing financial crimes laws. The National Accountability Bureau (NAB), the Anti-Narcotics Force (ANF), the Federal Investigative Agency (FIA), and the Directorate of Customs Intelligence and Investigations (CII)—re-designated as the "Directorate General, Intelligence & Investigations" (FBR)—all oversee Pakistan's financial enforcement efforts. The FIU has also established a Special Investigation Group to investigate terrorism and terrorism financing. In addition to the 2007 Anti-Money Laundering Ordinance, major laws in these areas include: The Anti-Terrorism Act of 1997, which defines the crime of terrorist finance and establishes jurisdiction and punishments; the National Accountability Ordinance of 1999, which requires financial institutions to report corruption related suspicious transactions to the NAB and establishes accountability courts; and the Control of Narcotics Substances Act of 1997 which criminalizes acts of money laundering associated with drug offenses and requires the reporting of narcotics related suspicious transactions. The present government has formed a committee to review the NAB ordinance (and the continuing viability of the NAB itself); however, the review process is still incomplete. The NAB, FIA, ANF and Customs have the ability to seize assets, whereas the SBP has the ability to freeze assets. The ANF shares information about seized narcotics assets and the number of arrests with the USG.

Pakistan has also adopted measures to strengthen its financial regulations and improve the reporting requirements for the financial sector to reduce its susceptibility to money laundering and terrorist financing. The SBP and the SECP are the country's primary financial regulators. They have established AML units to enhance financial sector oversight. However, these units often lack defined jurisdiction and adequate resources to effectively supervise the financial sector on AML/CTF controls. The SBP has introduced regulations on AML that are generally consistent with the FATF recommendations in the areas of "know your customer" and enhanced due diligence procedures, record retention, the prohibition of shell banks, and the reporting of suspicious transactions. The Securities and Exchange Commission of Pakistan, which has regulatory oversight for nonbank financial institutions, has also applied "know your customer" regulations to stock exchanges, trusts, and other nonbank financial institutions. However, there is no designated AML/CTF supervisor for designated nonfinancial businesses and professions.

Pakistan has specifically criminalized various forms of terrorist financing under the Anti-Terrorism Act (ATA) of 1997. Sections 11H-K provide that a person commits an offence if he is involved in fund raising, uses and possesses property, or is involved in a funding arrangement intending that such money or other property should be used, or has reasonable cause to suspect that they may be used, for the purpose of terrorism. Pakistan has the ability to freeze bank accounts and property held by terrorist individuals and entities. The ATA of 1997 also allows the government to proscribe a fund, entity, or individual on the grounds that it is involved with terrorism. This done, the government may order the freezing of its accounts. Section 11B of the ATA specifies that an organization is proscribed or listed if the GOP has reason to believe that it is involved with terrorism.

Pakistan has issued freezing orders for terrorists' funds and property in accordance with UN Security Council Resolutions 1267 and 1373. The SBP circulates to its financial institutions the list of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list. Since 2001, a total of PKR 752 million (approximately $9.6 million) has been frozen under UN Security Council Resolutions 1267 and 1373. However, there have been some deficiencies concerning the timeliness and thoroughness of the asset freezing. There are sometimes delays in the transmission of information about asset freezing to relevant agencies such as the Finance Ministry and the SBP, which reduces the effectiveness of the implementation of these resolutions. The State Bank, however, maintains that as soon as it receives the information about these resolutions, it instructs banks to freeze these assets.

The Bank's most recent freeze orders have involved Jamatt ud Dawa (JUD), the organization connected with the November 2008 Mumbai attacks. The JUD is a reinvention of the Lashkar-e-Taiba (LeT), which originally was designated as a terrorist organization by the United States in December 2001, was banned by Pakistan in January 2002, and added to the UNSCR 1267 list in 2005. The reinvention as JUD was a specific effort by the group to avoid sanctions, but in December 2008, the UNSC added additional JUD aliases to its 1267 list, listed four members of LeT to its 1267 list for targeted sanctions and added aliases for Al Rashid and Al Akhtar Trusts, which raise funds for LeT. JUD continues to use LeT's vast network of mosques, hospitals, clinics, madrassas and fundraising offices throughout Pakistan to raise money and recruit on behalf of LET

A Charities Registration Act has been under consideration by the Ministry of Welfare for some time. It was sent to the Economic Affairs Division of the Ministry of Finance, which returned the draft text with their comments to the Ministry of Social Welfare. The Ministry of Social Welfare will now forward the bill to the Ministry of Law for review. The bill will then require approval by the cabinet and National Assembly, unless issued as a Presidential Ordinance by the President. Under this bill, charities would have to prove the identity of their directors and open their financial statements to government scrutiny. Currently, charities can register under one of a dozen different acts, some dating back to the middle of the nineteenth century. The Ministry of Social Welfare hopes that when the new legislation is enacted, it will be better able to monitor suspicious charities and ensure that they have no links to designated terrorists or terrorist organizations.

Current efforts to crack down on the flow of illicit funds via charitable organizations are limited to closure of the charity. There is little follow-up on suspect individuals associated with charities in question, thus allowing them to operate freely under alternate names. The court system has also failed to affirm Pakistan's international obligations and maintain closure of UN-proscribed charitable organizations. In one such case, a provincial court in Karachi permitted a charity to continue operating in the face of a closure order, provided the charity in question only engage in humanitarian operations. The GOP failed to aggressively appeal this court decision.

Reportedly, bulk cash couriers are the major source of funding for terrorist activities. According to the Pakistan Central Board of Revenue, cash smuggling is an offense punishable by up to five years in prison. The SBP legally allows individuals to carry up to $10,000 in dollars or the foreign currency equivalent. In tracking the cross border movement of currency, Pakistan currently has reporting requirements only for the exportation of currency not the importation of currency. Therefore, Pakistan is only partially in compliance with FATF's Special Recommendation IX, as they have no declaration or disclosure system for incoming currency. Officials are able to ask anyone entering Pakistan if they are bringing in any currency. There are joint counters at international airports staffed by the SBP and Customs to monitor the transportation of foreign currency. As a result of cash courier training, their efforts to stop and seize the illicit cross-border movement of cash have increased. For example, during 2008 authorities made a number of significant cash seizures at the international airports in Karachi, Lahore, and Peshawar as well as land border crossings.

Pakistan is party to the 1988 UN Drug Convention and the UN Convention against Corruption. Pakistan has signed but not ratified the UN Convention against Transnational Crime, and is not a party to the UN Convention for the Suppression of the Financing of Terrorism. Pakistan does not have a mutual legal assistance treaty with the United States. Pakistan is ranked 134 of 180 countries monitored in Transparency International's 2008 Corruption Perception Index.

Although the Government of Pakistan adopted a long-awaited AML Ordinance by presidential decree after years of delay and stall tactics, the ordinance does not meet international standards. Proposed revisions to the AML Ordinance designed to incorporate APG recommendations and correct deficiencies have now been put forward by the government, but the precise content and effect of those revisions remains closely held by the government, and is as of yet unknown. The Pakistani parliament must still pass the revised ordinance. Pakistan's Financial Monitoring Unit (FMU) needs to be strengthened and should be given operational autonomy rather than be subject to the supervision and control of the General Committee, which is comprised of political ministers. The GOP should also issue implementing regulations to consolidate and de-conflict the reporting obligations of suspicious transactions contained in various laws and regulations. Regular suspicious-transaction reporting, to include those that deal with terror financing, must become institutionalized as a banking practice, and the FMU must develop collection and analytical capacity. Pakistani law enforcement should not, however, become dependent on these reports to initiate investigations; rather, law enforcement authorities should be proactive in pursuing money laundering in their field investigations. In light of the role that private charities have played in terrorist financing, Pakistan must work quickly to conduct outreach, supervise, and monitor charitable organizations and activities, and close those charitable organizations that finance terrorism. In accordance with FATF Special Recommendation IX, Pakistan should implement and enforce cross-border currency reporting requirements and focus greater efforts in identifying and targeting illicit cash couriers. Pakistan should also become a party to the UN Convention against Transnational Organized Crime and the UN Convention for the Suppression of Terrorist Financing.

Palau

Palau is an archipelago of more than 300 islands in the Western Pacific with a population of 19,907 (more than 3,500 of which are foreign guest workers) and per capita GDP of approximately $8,412 (a large percentage of which comes from international financial assistance).

Upon its independence in 1994, the Republic of Palau entered the Compact of Free Association with the United States. The U.S. dollar is the legal tender used by the country, though it is not the official currency of Palau. Palau is not a major financial center. Nor does it offer offshore financial services. There are no offshore banks, securities brokers/dealers or casinos in Palau. Palauan authorities believe that drug trafficking, human trafficking, and prostitution is the primary sources of illegal proceeds that are laundered.

In January 2005, Palau prosecuted its first ever case under the Money Laundering and Proceeds of Crimes Act (MLPCA) of 2001 against a foreign national engaged in a large prostitution operation. The defendant was convicted on all three counts as well as a variety of other counts. Subsequently, Palau has prosecuted three more money laundering cases obtaining convictions in two of the cases. Two of the cases involved domestic proceeds of crime, while one of the cases involved criminal conduct both within and outside of Palau.

Amid reports in late 1999 and early 2000 that offshore banks in Palau had carried out large-scale money laundering activities, a few international banks banned financial transactions with Palau. In response, Palau established a Banking Law Review Task Force that recommended financial control legislation to the Olbill Era Kelulau (OEK), the national bicameral legislature, in 2001. Following that, Palau took several steps toward addressing financial security through banking regulation and

supervision and putting in place a legal framework for an anti-money laundering regime. Several pieces of legislation were enacted in June 2001.

The Money Laundering and Proceeds of Crimes Act (MLPCA) of 2001 criminalized money laundering and created a financial intelligence unit. Two years after the introduction of proposed amendments, an amended MLPCA was signed into law on December 19, 2007. The report of the mutual evaluation (MER) of Palau, conducted in 2008 jointly by the IMF and the Asia/Pacific Group on Money Laundering (APG) of which Palau has been a member since 2002, noted that deficiencies that the amended MLPCA does not cover the AML/CTF preventive measures in a satisfactory manner. Significant deficiencies remain in the areas of customer due diligence (CDD), record keeping, monitoring of transactions, and supervision. The Financial Institutions Commission (FIC) is the AML/CTF supervisor, but it does not have the resources to ensure AML/CTF compliance nor to issue any regulations. The designated nonfinancial businesses and professions (DNFBPs) operating in Palau are not covered by the MLPCA. The MER also noted that amended MLPCA did not increase the number of predicate crimes for money laundering to include the minimum 20 predicate crimes prescribed by the Financial Action Task Force (FATF). The Pacific Anti-Money Laundering Program's (PALP) Legal Mentor will continue to assist Palau in addressing legal and regulatory deficiencies relating to Palau's anti-money laundering regime.

The original act did not establish requirements for the recording of cash and bearer securities transactions of U.S. $10,000 and above, and only required the reportage of suspicious transactions in excess of U.S. $10,000. The MLPCA did mandate that records be kept for five years from the date of the transaction. All such transactions (domestic and international) are required to go through a credit or financial institution licensed under the laws of the Republic of Palau. Credit and financial institutions are required to verify customers' identity and address. In addition, these institutions are required to check for information by "any legal and reasonable means" to obtain the true identity of the principal/party upon whose behalf the customer is acting. If identification cannot be confirmed, the transaction must cease immediately.

The amended MLPCA, in addition to generally tightening up the original law, now sets higher standards for record keeping, requires the recording of cash and bearer securities transactions in excess of U.S. $10,000, removes the dollar threshold on suspicious transactions and requires "alternative remittance systems" to be licensed and maintain records of all transactions in excess of U.S. $1,000. The amendment also requires currency transactions over U.S. $5,000 to be effected by wire transfer and also authorizes the Financial Institutions Commission (FIC) to conduct random compliance audits on credit or financial institutions. Palau also monitors cross border transportation of currency through a declaration form requiring travelers to declare U.S. $10,000 or more.

The MLPCA defines offenses of money laundering as: 1) conversion or transfer of property for the purpose of concealing its illegal origin; 2) concealing or disguising the illegal nature, source, location, disposition, or ownership of property; and 3) acquisition, possession, or control of property by any person who knows that the property constitutes the proceeds of crime as defined in the law. The law provides for penalties of a fine not less than U.S. $5,000, nor more than double the amount the convicted individual laundered or attempted to launder, whichever is greater, or imprisonment of not more than 10 years, or both. Corporate entities or their agents are subject to a fine double that specified for individuals. The law protects individuals who report suspicious transactions.

The Financial Institutions Act of 2001 established the Financial Institutions Commission (FIC), an independent regulatory agency, which is responsible for licensing, supervising and regulating financial institutions, defined as banks and security brokers and dealers in Palau. An amendment intended to strengthen the supervisory powers of the FIC and promote greater financial stability within Palau's banking sector passed its first reading in the Senate in January 2005. The Senate Committee on Ways and Means and Financial Matters did not report out the bill until December 2006 when it merely

referred it back to the Committee for further study. This amendment still has not become law. The insurance industry is not currently regulated by the FIC. Most insurance companies in Palau are companies registered in the U.S. or the U.S. Territory of Guam.

The Free Trade Zone Act of 2003 created the Ngardmau Free Trade Zone (NFTZ). A public corporation, Ngardmau Free Trade Zone Authority, was established to oversee the development of the NFTZ. The Authority also issues licenses for businesses to operate within the free trade zone. Businesses licensed to operate within the free trade zone will not be subject to the requirements of the Foreign Investment Act and will be exempt from certain import and export taxes. No development has taken place within the area designated for the free trade zone and the NFTZ directors continue to search for developers and investors.

Currently there are seven licensed banks in Palau, the majority ownership of which is primarily foreign. The three largest retail banks—Bank of Hawaii, Bank of Guam and BankPacific are all branches of American banks. In addition there are three banks chartered in Palau (Asia Pacific Commercial Bank, First Fidelity Bank and Palau Construction Bank) and one chartered in Taiwan (First Commercial Bank.)

On November 7, 2006, the FIC closed the second largest and the only locally owned bank, Pacific Savings Bank (PSB), for illiquidity and insolvency. The Receiver and the Attorney General filed a number of civil and criminal actions against former bank managers and insiders. An additional five to ten cases are currently being prepared. Investigations and litigation, though hampered by lack of resources, continue.

In October 2008, the Office of the Attorney General charged a Palauan and Taiwan businessmen for violations of foreign investment law, tax law, and money laundering. The Taiwan businessman operated three businesses listed under the name of his Palauan partner. Investigation into the records and confiscated receipts from the three companies suggest that income was grossly underreported over several years. A judge has issued an order to freeze bank accounts of the Taiwan businessman. The judge also ordered that no capital shall be removed and no financial transaction to be conducted.

With the legal framework now being made more robust, the weakest link in Palau's money laundering prevention regime is the paucity of human and fiscal resources. Palau has an Anti-Money Laundering Working Group comprised of the Office of the President, the FIC, the Office of the Attorney General, Customs, the FIU, Immigration, and the Bureau of Public Safety. However, the operations of the government's Financial Intelligence Unit (FIU) has been severely restricted by a lack of dedicated human resources and no dedicated budget. In December 2008, the Palauan government agreed to allocate a budget for a full time Director of the FIU. The FIU, will still be under the FIC, is responsible for receiving, analyzing, and processing suspicious transaction reports, and disseminating the reports as necessary. In addition, the FIU is responsible for tracing, seizing, and freezing assets. To accomplish this with the limited manpower available a multi-agency SAR review team was organized with the assistance of the PALP mentor to jointly review information collected by the FIU to identify and initiate investigations. The multi-agency approach has enabled the FIU to function given its limitations of manpower and funding and has fostered information sharing and joint investigations between the relevant law enforcement agencies. Another impediment to enforcement is the lack of implementing regulations to ensure compliance with the amended MLPCA. Regulations have been drafted to address these deficiencies identified in the MER and are expected to be passed in 2009.

Palau has enacted several legislative mechanisms to foster international cooperation. The Mutual Assistance in Criminal Matters Act (MACA), passed in June 2001, enables authorities to cooperate with other jurisdictions in criminal enforcement actions related to money laundering and to share seized assets. The Foreign Evidence Act of 2001 provides for the admissibility in civil and criminal proceedings of certain types of evidence obtained from a foreign state pursuant to a request by the Attorney General under the MACA. Under the Compact of Free Association with the United States, a

full range of law enforcement cooperation is authorized and in 2004 Palau was able to assist the Department of Justice in money laundering investigation by securing evidence critical to the case and freezing the suspected funds. Palau has also entered into an MOU with Taiwan and the Philippines for mutual sharing of information and interagency cooperation in relation to financial crimes and money laundering.

In 2004 the President also sent the Cash Courier Disclosure Act, drafted by the Palau Anti-Money Laundering Working Group, to the legislature. The bill, intended to strengthen the FIC, was signed into law in May 2007. The law mandates a written declaration with the Division of Customs for $10,000 or more in cash or negotiable instruments that is transported in or out of the country. An administrative penalty of 5 percent of the amount of the currency transported may be assessed for failure to file a declaration; the civil penalty against any person shall not exceed twice the amount of the currency being illegally transported. Penalties for entities shall equal two times the fines specified for natural persons. Entities found guilty of three or more offenses within a five-year period may be banned from business activities for a minimum of five years, or ordered to close permanently; such judgments will be publicized in the press. The Cash Courier Disclosure Act included an amendment for the Attorney General to bring civil suit against entities or persons who attempt to or engage in banking business, the brokerage or dealing of securities, without a valid license from the FIC. A person who commits the offense shall be penalized at least $25,000; corporate entities are fined an amount equal to two times the fine for a natural person, or the amount of gross profit realized by the entity for the two years prior to the offense, whichever is greater. Such entities may be banned from business activities for a minimum of five years, or ordered to close permanently, such judgment to be publicized in the press. The PALP Law Enforcement resident mentor has trained and worked with Palau Customs, Police and Airport Security to identify potential bulk cash smugglers and the methods they employ. Since the passage of the Cash Courier Disclosure Act, Palau Customs/Security have identified and made six separate bulk cash currency seizures of nearly $100,000 at the airport in 2008.

Palau is a party to the UN Convention for the Suppression of the Financing of Terrorism. The Counter-Terrorism Act of 2007 (CTA includes provisions for the freezing of assets of entities and persons designated by the United Nations as terrorists or terrorist organizations, provisions for the regulation of nonprofit entities to prevent abuses by criminal organizations and terrorists, and provisions for criminalizing the financing of terrorism. The Counter-Terrorism Act specifically addresses Palau's obligation under UN Security Council Resolution 1373. However, the 2008 MER stated that Palau's legislation does not adequately address provisional measures of seizing of evidence and property and the freezing of capital and financial transactions related to the financing of terrorism. Palau is not a party to the 1988 UN Drug Convention, the UN Convention against Corruption, or the UN Convention against Transnational Organized Crime.

Under Palau law, donations over U.S. $5,000 to any nonprofit organization are to be recorded. The organization must maintain the record for 3 years and must provide it to the FIU upon request. Donations over U.S. $10,000 are to be reported to the Office of the Attorney General and FIU. Any suspicious donations are also to be reported to the Office of the Attorney General and FIU. Penalties for violations are: a fine not to exceed U.S. $10,000; a temporary ban on operations for up to 2 years; or the dissolution of the organization.

The Government of Palau (GOP) has taken several steps toward enacting a legal framework by which to combat money laundering. The GOP should circulate the UNSCR 1267 Sanctions Committee Consolidated list of terrorist entities. The GOP should provide more resources to its FIU, to ensure that it can fulfill its mission. The GOP should extend its excellent monitoring of airport to all its border points of entry and exit to protect against the smuggling of bulk cash, narcotics and other contraband and should implement all aspects of the legal reforms already in place. Palau should also address the deficiencies noted in its recent mutual evaluation report to ensure that it continues to make progress in developing a viable anti-money laundering/counterterrorist financing regime that comports with

international standards. Palau should also become a party to the 1988 UN Drug Convention, the UN Convention against Corruption and the UN Convention against Transnational Organized Crime

Panama

Panama is an important regional financial center and has had one of the fastest growing economies in the Western Hemisphere over the past 15 years. GDP growth was 11 percent in 2007, 9.2 percent in 2008, and projected by the United Nations to be 4.5 percent in 2009. However, the very factors that have contributed to Panama's economic growth and sophistication in the banking and commercial sectors—the large number of offshore banks and shell companies, the presence of the world's second-largest free trade zone, the spectacular growth in ports and maritime industries, and the use of the U.S. dollar as the official currency—also provide an effective infrastructure for significant money laundering activity. The majority of money laundering activity in Panama is narcotics-related or the result of transshipment or smuggled, pirated, and counterfeit goods through Panama's major free trade zone, the Colon Free zone (CFZ). The funds generated from illegal activity are susceptible to being laundered through a wide variety of methods, including the Panamanian banking system, Panamanian casinos, bulk cash shipments, pre-paid telephone cards, debit cards, insurance companies, real estate projects and agents, and merchandise. Panama's vulnerability to money laundering is exacerbated by the government's lack of adequate enforcement, personnel, and resources devoted to anti-money laundering and combating the financing of terrorism (AML/CTF), as well as the sheer volume of economic transactions, a significant portion of which is in cash).

Panama's economic and geographic proximity to drug-related activity from Colombia, Venezuela, and Mexico, as well as weak capacity within the Government of Panama (GOP), makes Panama a natural location for money laundering. The principal source of laundered money is derived from the sale in the United States and Europe of cocaine produced in Colombia. Panama's land border with Colombia is approximately 60 miles of unguarded dense jungle. Sea and air law enforcement of its borders is often ineffective.

Panama, particularly in the CFZ, also suffers from substantial transshipment of smuggled or pirated goods, including counterfeit apparel, pharmaceuticals, and pirated DVDs. In 2008 alone, the CFZ imported and exported over $18 billion in goods and the CFZ is the world's second largest free trade zone after Hong Kong. The CFZ currently has over 2,786 businesses, 25 bank branches (including money center banks such as Citibank and HSBC), employs approximately 29,100 people, and continues to expand. The large volume of international business within the CFZ provides a possible environment for money laundering by individuals raising or moving funds on behalf of terrorist groups. Exacerbating the vulnerabilities of the CFZ is a legal staff of only three attorneys to oversee transshipment, smuggling of goods, counterfeit products and intellectual property violations issues.

The CFZ offers a unique set of advantages that promote business activities, including exemption from Panamanian taxes and the associated financial controls; serving as a one-stop shop for importing, financing, and shipping goods; serving as a showroom for East Asian goods; providing rapid transfer of goods with three ports along with a road, railroad, and canal to ports and airports on the Pacific; and offering cheap financing in a large financial sector that uses U.S. dollars. Criminal merchants and customers are able to use these legitimate advantages to facilitate money laundering activities. Highlighting the challenges of enforcement in the face of large trade volumes is the case of Ricardo Traad, the former Administrator of Panamanian Maritime Service (akin to the U.S. Coast Guard), who was arrested in 2007 for, among other things, money laundering and narcotics trafficking. In addition to the CFZ, Panama also had fifteen export processing zones at the end of 2007 and the ports of Panama handle over four million twenty-foot equivalent units (TEUs) of container traffic per year.

Panama is an offshore financial center that includes offshore banks and various forms of shell companies that have been used by a wide range of criminal groups globally for money laundering. The

Panamanian Superintendent of Banks licenses offshore banks and the Public Registry facilitates the formation of offshore corporations. Business licenses may be obtained through a newly created online system. The Superintendent of Banks requires a list of a bank's shareholders as part of the licensing process. The onshore and offshore registration of corporations is also handled by the Public Registry.

As of September 2008, Panamas had 90 commercial banks, two official banks, 15 local banks of general license, 28 foreign banks of general license, 33 banks of international license, and 14 representative offices. Of the 90 commercial banks in Panama, 73 are specifically either non-Panamanian or are designed to service offshore clients. Approximately 46,178 and 40,825 new offshore corporations were registered in Panama during 2007 and through October 2008, respectively. Panama also has a thriving financial and legal services industry directed at providing offshore tax planning, estate planning, and trust organization services. Panama does not tax individuals or companies on non-Panamanian sources of income and maintains neither exchange controls nor restrictions on capital flows. Further, there is no requirement to disclose the beneficial owners of any corporation or trust. Bearer shares are permitted for corporations, and nominee directors and trustees are allowed by law. Panama regulates gaming activities in-country, but does not regulate Internet gaming sites.

Panama's construction sector, which is growing at double-digit rates, is an emerging industry of concern for money laundering. It has been fueled by a booming domestic economy along with an influx of foreigners, particularly Colombians, Venezuelans, North Americans, and Europeans. The construction sector in Panama often pays employees and suppliers in cash, which increases its attractiveness to money launderers. For instance, the developer of one residential project (Resort Paraiso Las Perlas on Isla Chapera in the Gulf of Panama), Jose Nelson Urrego Cardenas, was arrested in 2007 on drug money laundering charges. The slowdown in the Panamanian construction sector due to the global slowdown indicates, however, that the construction sector may be primarily based upon legitimate commerce.

Panama has a comprehensive legal framework to detect, prevent, and combat money laundering and terrorist financing, and provides excellent cooperation with U.S. law enforcement agencies in combating drug trafficking, money laundering and financial crimes. The GOP identified the combating of money laundering as one of five goals in its five-year National Drug Control Strategy, issued in 2002, and commits the GOP to devoting $ 2.3 million to anti-money laundering projects, the largest being institutional development of the GOP's financial intelligence unit (FIU), the Unidad de Análisis Financiero (UAF).

Money laundering is a criminal offense in Panama. Law 14 (Article 284) of May 17, 2007, amends the Penal Code by expanding the predicate offenses for money laundering beyond narcotics trafficking to include criminal fraud, arms trafficking, trafficking in humans, kidnapping, extortion, embezzlement, corruption of public officials, terrorism, and international theft or trafficking of motor vehicles. Law 14 establishes a five to 12 year prison sentence, plus possible fines. Additionally, the Panamanian Legislative Assembly approved the Financial Crimes Bill (Law No. 45 of June 4, 2003), establishing criminal penalties of up to ten years in prison and fines of up to $1 million for financial crimes that undermine public trust in the banking system, the financial services sector, or the stock market. The legislation criminalizes a wide range of activities related to financial intermediation, including illicit transfers of monies, accounting fraud, insider trading, and the submission of fraudulent data to supervisory authorities. Law No. 1 of 2004 also adds crimes against intellectual property as a predicate offense for money laundering.

Panama's Law 16 of 1982, Article 389, and Law 50 of 2003, Article 264, both criminalize the financing of terrorism as contemplated by UN Security Council Resolution 1373. Decree No. 22 of June 2003, gave the "Presidential High Level Commission against Narcotics Related Money Laundering" responsibility for combating terrorist financing. Law No. 50 of July 2003 criminalizes

terrorist financing and gives the UAF responsibility for prevention of this crime. By means of Law No. 22 of May 2002, the GOP adopted the UN Convention for the Suppression of the Financing of Terrorism. Panama also circulates to its financial institutions the list of individuals and entities included on the UN 1267 Sanctions Committee consolidated list.

Under Panamanian customs regulations, any individual bringing cash in excess of $10,000 into Panama must declare such monies at the point of entry. If such monies are not declared, they are confiscated and are presumed to relate to money laundering.

Under Panamanian law and regulations, financial institutions (banks, trust companies, money exchangers, credit unions, savings and loans associations, stock exchanges and brokerage firms, and investment administrators) must adhere to "know your customer" (KYC) practices for identification of customers, exercise of due diligence, and retention of transaction records. Executive Decree No. 52 of April 30, 2008, referred to as the "New Banking Law," states that banks and other supervised entities are obliged to establish policies, procedures, and controls on the prevention of money laundering, terrorist financing, and related crimes. Financial institutions must also examine every cash (or cash equivalent) transaction in excess of $10,000 or a series of transactions that in the aggregate exceed $10,000 in any given week, as well as any transaction, regardless of its amount, that could be related to money laundering activity.

The Superintendent of Banks supervises and examines financial institutions for compliance with anti-money laundering and combating the financing laws and regulations, including for compliance with KYC policies on banks and other supervised entities. There are no differing regulations governing onshore and offshore corporations. Panamanian trust companies are required to identify to the Superintendent of Banks the beneficial owners of trusts. Panamanian law provides for the dissemination of information related to trusts to appropriate administrative and judicial authorities.

Financial institutions must report currency transactions in excess of $10,000 and suspicious financial transactions to the UAF. Panamanian law protects reporting individuals (banks and others) from civil and criminal suits with respect to providing information required by law. Casinos, CFZ businesses through the CFZ Administration, pawnshops, the national lottery, real estate agencies and developers, and insurance and reinsurance companies also report to the UAF currency transactions that exceed $10,000. Financial institutions are prohibited from informing their client or third parties that they have transmitted any information regarding such transactions to the UAF. Panamanian law requires all financial institutions to maintain for five years records concerning their anti-money laundering procedures, including information regarding their customers and any information derived as part of the KYC regulations or suspicious transactions reports relating to customer identification.

AML/CTF controls are applied to numerous nonbanking financial institutions in Panama. Article 248 of 2000 requires indigenous alternative remittance systems, such as hawala operations, to adhere to the reporting requirement for cash transactions. The Ministry of Commerce and Industry is responsible for supervising money remittance houses, financing companies, real estate promoters and agents, pawnshops, and companies located in enterprise processing zones. Executive Decree 524 promulgated on October 31, 2005 (amended by Executive Decree 627 of 2006), establishes a procedure to regulate, supervise and control nongovernmental organizations, including charities. The preamble to Executive Decree 524 mentions Law 50 of 2003 and the need to regulate such organizations to combat terrorism and prevent terrorist financing. Press reports, however, have questioned the degree to which the nongovernmental organizations are complying with their reporting and registration requirements.

The Panamanian Autonomous Cooperative Institute supervises savings and loan cooperatives. It has established a specialized unit for the supervision of loans and credit cooperatives regarding compliance with Law 42. The National Securities Commission supervises securities firms, stockbrokers, stock exchanges and investment managers. The commission carries out various training sessions and workshops for its personnel and related entities. The National Lottery of Public Welfare

supervises activity related to the sale of lottery tickets and payments of winnings. The Gaming Commission supervises casinos, horse tracks and other establishments dedicated to betting and games of chance. The Superintendence of Insurance supervises insurance companies, reinsurance companies, and insurance brokers. The CFZ Administration supervises the companies and activity within the CFZ and has actively sought to address CFZ vulnerabilities to illicit behavior, such as money laundering. The CFZ Administration mandates the training of representatives of all CFZ businesses in money laundering and counterterrorist financing laws. Noncompliance with these laws can result in fines of up to $1 million. The CFZ Administration also issues a procedures manual for all CFZ businesses, outlining their responsibilities regarding the prevention of money laundering.

The GOP established the UAF in 1995. The UAF is the agency responsible for receiving and analyzing financial data and transactions received from financial and other institutions (public or private), including reports of suspicious activity which may be related to money laundering or terrorist financing. The UAF falls under the jurisdiction of the GOP's Council for Security and National Defense within the Ministry of the Presidency. Among its stated purposes is preventing the laundering of funds derived from narcotics trafficking, but it does not have criminal investigative responsibilities. The UAF's staff is comprised of personnel specialized in finance, law, and data processing. UAF personnel also participate with regulators drafting legislation.

The UAF has no online access to information of financial institutions unless such information is requested in writing. The only exception is with the Asociación Panameña de Crédito—(APC—the Panamanian Credit Association) for credit records. There is a formal mechanism in place to share information domestically. UAF has online access with other GOP entities such as the public registry, traffic department, electoral tribunal, and immigration movements as well as Customs travelers' declarations. Executive Decree No. 163 authorizes the UAF to share information with FIUs of other countries, subject to entering into a memorandum of understanding or other information exchange agreement. The UAF has signed more than 43 memoranda of understanding with FIUs from other countries, including the U.S. Financial Crimes Enforcement Network (FinCEN). The UAF also has online access to financial information with foreign analogs through the Egmont Secure Web.

Other UAF duties include maintaining statistics on the movement of cash within the country believed to be related to money laundering or terrorist financing, sharing information with the FIUs of other countries, and assisting the Attorney General's and Bank Superintendent's offices with their investigations relating to money laundering and terrorist financing. The UAF also works with other GOP agencies to identify new methods of money laundering and participates in the training of financial and nonfinancial sector employees in detecting and preventing money laundering. During 2008, the UAF trained 1,128 individuals from 31 institutions, including the Gaming Board, the Bar Association, the Ministry of Commerce, the Judicial Branch, credit unions, banks, remittances houses, insurance companies and CFZ businesses.

The UAF consists of approximately 20 to 25 employees. During 2007, the UAF reinforced the analysis department with two new accountants, a financial analyst, and a lawyer. Also, the statistics and typology departments have newly trained personnel. Despite these additions, the UAF is overworked and lacks adequate resources. After the UAF reviews the cash transaction reports (CTRs) and suspicious transaction reports (STRs) and gathers any other relevant information from reporting institutions and other government agencies, the UAF provides information related to possible money laundering or terrorist financing to the Office of the Attorney General for investigation. Money laundering cases involving narcotics are handled by the Drug Prosecutor's Office within the Office of the Attorney General. The Directorate of Judicial Investigations (similar in function to the U.S. Federal Bureau of Investigation) provides expert assistance to the prosecutors. The UAF routinely transfers cases to the financial investigations unit of the Directorate of Judicial Investigations.

Panamanian Customs continued a program at Tocumen International Airport to deter currency smuggling by seizing and forfeiting all undeclared funds in excess of $10,000 from arriving passengers. However, the entry of Customs currency declaration information into the UAF database has yet to occur, although discussed since 2002. In 2008, ICE and Customs authorities in Panama conducted joint interdiction operations in furtherance of ICE's Operation Firewall. Operation Firewall is a comprehensive law enforcement effort focusing on the interdiction and investigation of bulk cash being smuggled around the world. The operations, conducted at Tocumen International Airport, resulted in twelve currency seizures totaling over $670,000.

From January to October 2008, the UAF investigated 1071 STRs (792 from banks, 242 from remittances houses, one from casinos, 14 from credit unions, 11 from financial institutions, three from government, and eight from stocks brokerages). As of July 2008, 151 of these reports were sent to the Attorney General's Office for further action and 104 were found with no merit. The UAF carried out 167 information requests through the Egmont Group and 151 judicial assistances through June 2008. Data on the total amount of cash transactions for 2008 are not yet available; however, the number and amount of cash transactions are expected to be at record levels due to high GDP and CFZ growth rates. Through October 2008, the UAF received 317,665 CTRs and the total cash amount reported during the first ten months of 2008 was approximately $8.3 billion.

Through October 2008, the Financial Fraud Prosecutor's office investigated 332 cases related to financial crimes. These included credit card fraud (261), bankruptcy (7), money laundering (4) and financial crimes (60). During the same time period the Special Drug Prosecutor Office reported 79 drug-related to money laundering arrests, as opposed to 48 through all of 2006.

Panamanian Law 38 of August 10, 2007, provides for the seizure of assets derived from criminal activity. Upon an arrest, assets are frozen and seized. The assets are released upon a judge's order to the defendant in the event of a dismissal of charges or acquittal. In the event of a conviction, assets derived from money laundering activity related to narcotics trafficking are delivered to the National Commission for the Study and Prevention of Narcotics Related Crimes (CONAPRED) for administration and distribution among various GOP agencies. Seized perishable assets may be sold and the proceeds deposited in a custodial account with the National Bank. Panamanian law provides for criminal forfeiture, but not civil forfeiture.

Responsibility for tracing, seizing and freezing assets lies principally with the Drug Prosecutor's Office of the Attorney General's Office. There are two offices in Panama province, one in each of the other provinces and one delegate in Darien province. The GOP typically enforces seizure and forfeiture laws fully in drug trafficking and money laundering cases. The banking sector is required by law to cooperate with the seizure and freezing of assets, and generally cooperates with law enforcement.

Although Panama does not have an independent national system or mechanism for freezing terrorist assets other than its current legislation, the Government of Panama does have dedicated financial crime positions to work these issues. Panama has not enacted any law for sharing seized assets with other governments. The Panama Public Force (PPF) and the judicial system have limited resources to deter terrorists, due to insufficient personnel and lack of expertise in handling complex international investigations. On January 18, 2003, the GOP entered into a border security cooperation agreement with Colombia, and also increased funds to the PPF to help secure the frontier.

Panama is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. Panama is a signatory to 11 of the UN terrorism conventions and protocols. Panama is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD), and is a member of the Caribbean Financial Action Task Force (CFATF). Panama is also a member of the Offshore Group of Banking Supervisors, and the UAF is a

member of the Egmont Group. Panama has hosted international conferences on money laundering. On August 9-10, 2007, the First International Congress on Handling Fraud and Corruption in the hemisphere was held in Panama which also included discussions on money laundering detection and prevention. The Banking Association/UAF/and other GOP entities organized the XII Hemispheric Congress on Prevention of Money Laundering and Combating the Financing of Terrorism August 2008

Panama and the United States have a Mutual Legal Assistance Treaty that entered into force in 1995. In March 2007, USG and GOP agencies cooperated in the largest maritime cocaine seizure known to have ever occurred. The seized vessel contained approximately 20 tons of cocaine, with an estimated market value of approximately $500 million. Authorities stopped the vessel "Gatun" off the Pacific coast of Panama.

Panama is involved in several other AML/CTF efforts. With support from the Inter-American Development Bank (IDB), the Government of Panama (GOP) is implementing a "Program for the Improvement of the Transparency and Integrity of the Financial System." The Program is targeted, through enhanced communication and information flow, training programs, and technology, at strengthening the capabilities of government institutions responsible for preventing and combating financial crimes and terrorist financing activities. Overall, 1,500 employees from 14 institutions have benefited from this training, including representatives of the private sector, stock markets, credit unions, bank compliance officials, and others. In addition, with the help of this program, Panama has launched an educational campaign to prevent money laundering and terrorist financing. The program began in 2002 and is intended to raise citizens' awareness of these crimes.

The GOP also created, within the Ministry of Foreign Affairs, the Department of Analysis and Study of Terrorist Activities. This department is tasked with working with the United Nations and the Organization of American States to investigate transnational issues, including money laundering. Panama has an implementation plan for compliance with the FATF Forty Recommendations on Money Laundering and Nine Special Recommendations on Terrorist Financing.

The GOP should continue its commendable efforts to enhance Panama's ability to prevent, detect, investigate, and prosecute financial crimes, including money laundering and terrorist financing. . The staff of the UAF, CFZ Administration, and GOP law enforcement entities should improve the level of enforcement, personnel, and resources devoted to AML/CTF, including successful prosecution of AML/CTF cases. As a member of CFATF, the GOP is committed to adhere to all FATF Recommendations, as well as those relating to the transparency of beneficial owners of all companies, including international business companies (IBCS). The issuance of bearer shares are of concern and the GOP should take adequate steps (such as immobilization) to assure that these instruments are not used for money laundering. The GOP should also enable the UAF and law enforcement users of the Public Registry's website to search by company officers names. The GOP should continue to implement transparency promoting computer systems that shine a light on CFZ commercial and financial transactions. Additionally, the GOP should devote more resources to ensuring that its CFZ does not serve to enable trade-based money laundering.

Paraguay

Paraguay is a principal money laundering center and major drug transit country involving the banking and nonbanking financial sectors. A multi-billion dollar contraband trade occurs in the border region shared with Argentina and Brazil, called the Tri-Border Area, and facilitates much of the money laundering in Paraguay. While the Government of Paraguay (GOP) suspects that proceeds from narcotics trafficking are often laundered in the country, it is difficult to determine what percentage of the total amount of laundered funds is generated from narcotics sales. Weak controls in the financial sector, open borders, bearer shares, casinos, a plethora of exchange houses, lax or non-enforcement of

cross border transportation of currency and negotiable instruments, and minimal enforcement activity for financial crimes allow money launderers, possible terrorist financiers, and transnational criminal syndicates to take advantage of Paraguay's financial system.

Ciudad del Este (CDE), on Paraguay's border with Brazil and Argentina, represents the heart of Paraguay's underground or "informal" economy. The area is well known for arms and narcotics trafficking and violations of intellectual property rights—and the illicit proceeds from these crimes are a source of laundered funds. A wide variety of counterfeit goods, including cigarettes, CDs, DVDs, and computer software, are imported from Asia and transported across the border into Brazil, with a smaller amount remaining in Paraguay for sale in the local economy. Some former government officials have been accused of involvement in the smuggling of contraband or pirated goods. Although there are ongoing criminal investigations, to date there have been few convictions for smuggling contraband or pirated goods.

Paraguay is particularly vulnerable to money laundering, as little personal background information is required to open a bank account or to conduct financial transactions. Paraguay is also an attractive financial center for neighboring countries, particularly Brazil. Foreign banks are registered in Paraguay and nonresidents are allowed to hold bank accounts, but current regulations forbid banks from advertising or seeking deposits from outside the country. While offshore banking in Paraguay is illegal, bearer shares are permitted—exposing the country to money laundering risk. A 2008 International Monetary Fund review of the GOP's anti-money laundering controls noted that a significant portion of corporations issue bearer shares and that no measures are in place to ensure that such entities are not being misused for money laundering. While casinos exist, offshore casinos do not, and Internet gambling is marginal, largely due to limited Internet connectivity throughout the country. Shell companies and trust funds structures are legal but seldom used and uncommon in the financial system. At present, the financial sector seems to lack the depth and sophistication to use these structures.

The nonbank financial sector operates in a weak regulatory environment with limited supervision. Credit unions or "cooperatives" are one of the main nonbank agents in the economy, rapidly growing in membership and representing over 20 percent of deposits and 33 percent of loans in the financial system. The organization responsible for regulating and supervising credit unions, the National Institute of Cooperatives (INCOOP), is an independent body that provides regulatory and supervisory guidelines, but lacks the capacity to enforce compliance. Exchange houses are another nonbank sector where enforcement of compliance requirements remains limited. By law, exchange houses need to register with the Central Bank. The Central Bank has the authority to intervene, close, and seize the assets of illegal exchange houses, and the Attorney General's office has the responsibility to enforce anti-money laundering laws. However, it is estimated that in CDE alone there are more than 100 illegal exchange houses. Unregistered exchange houses are highly susceptible to money laundering activity, and in CDE they are associated with laundering funds from illicit activity.

In July 2008, President Duarte Frutos signed a new penal code that includes enhanced legislation on money laundering. Under the new penal code money laundering is an autonomous crime, punishable by a prison term of up to five years. The new code establishes predicate offenses for money laundering but does not require a conviction for the predicate offense before initiating money laundering charges. The new code also allows the state to charge financial sector officials who negligently permit money laundering to occur. Implementation of the new penal code is expected for mid-2009 to allow time for judge and prosecutor training.

Another bill amending Paraguay's criminal procedure code is expected in 2009. The proposed amendments to the criminal procedure code would move Paraguay toward a more accusatory system. The reforms would allow criminal investigations to occur without advance notice of the investigation

to the subject or the defense attorney, lengthen statutes of limitation, and allow for confrontation and cross examination of witnesses.

Paraguay does not have laws that criminalize terrorist financing or would provide authorities to freeze, seize, or forfeit assets related to the financing of terrorism. Efforts to include such statutes in the new penal code failed. The Ministry of Industry and Commerce's (MIC) Secretariat to Combat Money Laundering (SEPRELAD) is working on a revised draft of the anti-terrorism finance bill to present to Congress in early 2009. The Egmont Group notified Paraguay about the need to comply with its international commitments regarding anti-terrorism finance legislation. If Paraguay does not show reasonable progress in enacting anti-terrorism finance legislation it could face suspension from the Egmont Group in 2009, which could then be followed ultimately by expulsion.

Other challenges slow Paraguay's progress in combating money laundering. Paraguay added three financial crimes prosecutors in 2007, bringing the total number to 11, but prosecutors still face resource constraints that limit their ability to investigate and prosecute financial crimes. New criteria were issued in 2005 for the selection of judges, prosecutors and public defenders; however, the process remains one that is largely based on politics, nepotism and influence peddling. Now that the new anti-money laundering legislation has been passed as part of the new penal code, it is critical to Paraguay's future prosecutorial successes that judges and prosecutors enhance their knowledge regarding the successful prosecution and adjudication of money laundering cases.

There are no effective controls or laws that regulate the amount of currency that can be brought into or out of Paraguay. Cross-border reporting requirements are limited to customs declaration forms issued by airlines at the time of entry into Paraguay. Persons transporting $10,000 into or out of Paraguay are required to file a customs report, but these reports are not collected or checked. Customs operations at the airports or land ports of entry provide no control of cross-border cash movements. The nonbank financial sector (particularly exchange houses) is used to move illicit proceeds both from within and outside of Paraguay into the U.S. banking system.

Most high-priced goods are paid for in U.S. dollars, and cross-border bulk cash smuggling is a major concern. Large sums of dollars generated from normal commercial activity and suspected illicit commercial activity are transported physically from Paraguay through Uruguay and Brazil to banking centers in the United States. The GOP is only beginning to recognize and address the problem of the international transportation of currency and monetary instruments derived from illegal sources.

Bank secrecy laws in Paraguay do not prevent banks and financial institutions from disclosing information to bank supervisors and law enforcement entities. Bankers and others, however, are protected under the anti-money laundering law with respect to their cooperation with law enforcement agencies. Banks, finance companies, insurance companies, exchange houses, stock exchanges and securities dealers, investment companies, trust companies, mutual and pension funds administrators, credit and consumer cooperatives, gaming entities, real estate brokers, nongovernmental organizations, pawn shops, and dealers in precious stones, metals, art, and antiques are required to know and record the identity of customers engaging in significant currency transactions. These entities must also report suspicious activities to Paraguay's financial intelligence unit (FIU), the Unidad de Análisis Financiera (UAF) within SEPRELAD. The Superintendence of Banks enforces these reporting obligations for banks, but they are not enforced for other financial institutions. In November 2007, the MIC issued new regulations that define reporting requirements and sanctions for noncompliance for the insurance industry and credit unions.

The government of Paraguay made significant efforts to strengthen SEPRELAD. Former Central Bank president Gabriel Gonzalez managed SEPRELAD until early August 2008. Director Gonzalez's efforts improved SEPRELAD's response time and operational structure, eliminating the backlog of suspicious activity reports (SARs). He also hired and trained additional UAF staff, strengthening the unit's analytical capacity. President Fernando Lugo's new administration designated in mid-August

Oscar Boidanich, a banking supervision and anti-money laundering veteran from the Central Bank, as SEPRELAD's new Director. Director Boidanich has worked to improve the quality of reported information in the SARs, and streamlined the information exchange processes with reporting institutions. In three months, SEPRELAD processed 276 SARs and sent 22 cases to the Attorney General's office, which represents a 20 percent increase over the same period in previous years.

SEPRELAD is hampered by a lack of effective inter-agency cooperation, as there is no formal mechanism for sharing sensitive information. Pursuant to a money-laundering vulnerability assessment performed in mid-2008 by the South America Financial Action Task Force (GAFISUD) and the International Monetary Fund (IMF), Director Boidanich is seeking to modify SEPRELAD's organizational structure to make it an independent secretariat with administrative and logistical support from the Central Bank with the aim of improving information-sharing mechanisms among the government's law enforcement agencies. SEPRELAD has drafted a bill, not yet pending before Congress, which would make it an independent secretariat reporting directly to the president. SEPRELAD is also seeking to strengthen its relationships with international counterpart financial intelligence units. Though Paraguay had long been in arrears with GAFISUD, it fully paid its outstanding dues in early 2008 and included the annual payment into its future budget requests. Paraguay has taken some measures to tackle illicit commerce and trade in the informal economy and to develop strategies to implement a formal, diversified economy.

Paraguay submitted a proposal for a second phase of the Millennium Challenge Corporation's Threshold Program to address corruption problems of impunity and informality, both of which hamper law enforcement efforts and contribute to money laundering. The Ministry of Industry and Commerce's Specialized Technical Unit (UTE), working in close coordination with the Attorney General's Trademarks and Intellectual Property Unit, seized $55 million worth of pirated goods during the first ten months of 2008. In cooperation with the U.S. Department of Homeland Security's Immigration and Customs Enforcement (ICE), the GOP continues to operate a Trade Transparency Unit (TTU) that examines discrepancies in trade data that could be indicative of customs or tax fraud, trade-based money laundering, or the financing of terrorism

Under current laws, enforcement agencies in Paraguay have limited authority to seize or forfeit assets of suspected money launderers. In most cases, assets seized or forfeited are limited to transport vehicles, such as planes and cars, and normally do not include bank accounts. However, law enforcement authorities may not auction off these assets until a defendant is convicted. At best, they can establish a "preventative seizure" (which has the same effect as freezing) against assets of persons under investigation for a crime in which the state risks loss of revenue from furtherance of a criminal act, such as tax evasion. However, in those cases the limit of the seizure is set as the amount of the suspect's liability to the government. In the past few years, Paraguay's anti-narcotics agency, SENAD, has been permitted on a temporary basis to use assets seized in pending cases, but SENAD cannot fully use such assets because the law does not permit the assets to be maintained or repaired. New asset forfeiture legislation is required to make improvements in this regard.

The law enforcement agencies have no authority to freeze, seize, or forfeit assets related to the financing of terrorism, which is not a criminal offense under Paraguayan law. The current law also does not provide any measures for thwarting the misuse of charitable or nonprofit entities that could be used as conduits for the financing of terrorism. However, the Ministry of Foreign Affairs provides the Central Bank and other government entities with the names of suspected terrorists on the UNSCR 1267 Sanctions Committee list.

The GOP has been slow to recognize terrorist financing within its borders. In December 2006, the U.S. Department of Treasury designated nine individuals and two companies operating in the Tri-Border Area as entities that provide financial and logistical support to Hezbollah. The nine individuals have all provided financial support and other services for Specially Designated Global Terrorist Assad

Ahmad Barakat, who was designated by the U.S. Treasury in June 2004 for his support to Hezbollah leadership. The two companies, Galeria Page and Casa Hamze, are located in Ciudad del Este and are used to generate or move terrorist funds. The GOP publicly disagrees with the designations, stating that the U.S. has not provided any new information that would prove terrorist financing activity occurs in the Tri-Border Area.

In spite of limitations in prosecuting suspected terrorist financiers such as Assad Ahmad Barakat and Kassem Hijazi, who were charged with tax evasion rather than terrorist financing or money laundering, the GOP is making improvements in its ability to successfully investigate and prosecute some money laundering cases. Leoncio Mareco was sentenced to 20 years in prison on August 14, 2007, for drug trafficking and money laundering. His wife, Zulma Rios de Mareco, was sentenced to 10 years in prison for money laundering. According to GOP authorities, the General Attorney's office has processed 40 money laundering cases, 15 of which resulted in convictions. These cases reinforce the fact that convictions are possible, although difficult, under the current legal framework.

Paraguay and the United States do not have a mutual legal assistance agreement; however, Paraguay is a party to the Inter-American Convention on Mutual Legal Assistance in Criminal Matters. Paraguay is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Corruption, and the UN Convention against Transnational Organized Crime. Paraguay is a member of the "3 Plus 1" Security Group with the United States and the Tri-Border Area countries. Paraguay is a member of GAFISUD, and SEPRELAD is a member of the Egmont Group.

The GOP took a number of positive steps in 2008 to combat money laundering, particularly with the passage of the new penal code and the money laundering convictions. However, it should continue to pursue other initiatives to increase its effectiveness in combating money laundering and terrorist financing. The GOP should enact legislation and issue regulations that comport with all international standards relating to its poorly regulated financial sector, and that enable law enforcement authorities to more effectively investigate and prosecute money laundering and terrorist financing cases. Paraguay should take steps to ensure that the penal and procedural code reforms are expeditiously approved and implemented, allowing for a more effective anti-money laundering regime. Paraguay does not have a counterterrorism law or a law criminalizing terrorist financing, and it should take steps as quickly as possible to ensure that comprehensive counterterrorism and counterterrorist financing legislation is introduced and adopted. It should also take the necessary steps to ensure that its TTU is comprised of vetted employees from all relevant agencies, including SEPRELAD. Further reforms in the selection of, and accountability by, judges, prosecutors and public defenders are needed, as are reforms to the customs agency to allow for increased inspections and interdictions at ports of entry and to develop strategies targeting the physical movement of bulk cash. Additionally, Paraguay should reform its asset forfeiture regime, including the management of seized and forfeited assets.

Peru

Peru is not a major regional financial center, nor is it an offshore financial center. Peru is the world's second largest producer of cocaine. Although no reliable figures exist regarding the exact size of the narcotics market in Peru, estimates indicate that the cocaine trade generates approximately two billion dollars annually, which is approximately 1.6 percent of Peru's gross domestic product. As a result, money laundering is believed to occur on a significant scale to integrate these illegal proceeds into the Peruvian economy. The most common methods of money laundering in Peru involve real estate sales, business investments, and high interest loans. Other vulnerabilities to money laundering include Peru's cash-based and heavily-dollarized economy, pervasive corruption, and the lack of effective regulatory supervision of nonfinancial businesses and professions, such as casinos and informal remittance and wire transfer services.

Money laundering has historically been facilitated by a number of factors, primarily Peru's cash-based economy. Peru's economy is heavily dependent upon the U.S. dollar. Approximately 60 percent of the economy is informal and approximately 65 percent is dollarized, allowing traffickers to handle large bulk shipments of U.S. currency with minimal complications. Currently, the Government of Peru (GOP) maintains no restrictions on the amount of foreign currency an individual can exchange or hold in a personal account, and until recently, there were no controls on bulk cash shipments coming into Peru. According to Peru's financial intelligence unit (FIU), the Unidad de Inteligencia Financiera (UIF), approximately 37 percent of money laundering cases have connections to criminal activity stemming from the drug trade.

Corruption remains an issue of serious concern in Peru. It is estimated that 15 percent of the public budget is lost due to corruption. Most recently, the Peruvian National Police Anti-Drug Directorate (DIRANDRO) arrested the Mayor of Pucallpa and 13 others on charges of money laundering drug trafficking proceeds through commercial enterprises. The nearly year-long investigation conducted by the police was assisted with reports from the UIF showing imbalances in the Mayor's business earnings. The Mayor owns a number of businesses in the region, which are now under asset seizure proceedings. The Mayor was formally indicted in October. Also, a number of former government officials, most from the Fujimori administration, are under investigation for corruption-related crimes, including money laundering. These officials have been accused of transferring tens of millions of dollars in proceeds from illicit activities (e.g., bribes, kickbacks, or protection money) into offshore accounts in the Cayman Islands, the United States, and Switzerland. The Peruvian Attorney General, a Special Prosecutor, the office of the Superintendent of Banks and Insurance, and the Peruvian Congress have conducted numerous investigations, some of which are ongoing, involving dozens of former GOP officials. In December 2007, Supreme Decree No. 085 created the National Office for Anti-Corruption (ONA). An anticorruption czar was appointed to a term of three years. In August 2008, however, the government closed the National Office for Anti-Corruption and transferred its responsibilities to the Comptroller's office.

Law 27.765 of 2002 criminalizes money laundering in Peru and expands the predicate offenses for money laundering to include the laundering of assets related to all serious crimes, such as narcotics trafficking, terrorism, corruption, trafficking of persons, and kidnapping. There does not have to be a conviction relating to the predicate offense. Rather, it must only be established that the predicate offense occurred and that the proceeds of crime from that offense were laundered. The law's brevity and lack of implementing regulations, however, limits its effectiveness in obtaining convictions.

Law 27.765 also revises the penalties for money laundering in Peru. Instead of a life sentence for the crime of laundering money, Law 27.765 sets prison terms of up to 15 years for convicted launderers, with a minimum sentence of 25 years for cases linked to narcotics trafficking, terrorism, and laundering through banks or financial institutions. In addition, revisions to the Penal Code criminalize "willful blindness," the failure to report money laundering conducted through one's financial institution when one has knowledge of the money's illegal source, and impose a three to six year sentence for failure to file suspicious transaction reports.

Law 29009, enacted in April 2007, granted temporarily to the Executive branch the power to legislate in the areas of illegal drug trafficking, money laundering, terrorism, kidnapping, extortion, and organized crime. The Executive branch enacted eleven legislative decrees prior to the law's expiration in July 2007 that strengthened the capacity of the National Police, the Public Ministry, and Executive branch to combat organized crime. Terrorism is considered a particular and long-standing problem in Peru, which is home to the terrorist organization Shining Path. Although the Shining Path has been designated by the United States as a foreign terrorist organization, and the United States and 100 other countries have issued freezing orders against its assets, the GOP has no legal authority to quickly and administratively seize or freeze terrorist assets. In the event that such assets are identified, the Superintendent for Banks must petition a judge to seize or freeze them and a final judicial decision is

then needed to dispose of or use such assets. Peru also has not yet taken any known actions to thwart the misuse of charitable or nonprofit entities that can be used as conduits for the financing of terrorism. Nongovernmental organizations are obliged to report the origins of their funds, according to UIF regulations.

Additionally, terrorism has not yet been specifically and fully established as a crime under Peruvian legislation in a manner that would conform to international standards. The only reference to terrorism as a crime is in Executive Order 25.475, which establishes the punishment of any form of collaboration with terrorism, including economic collaboration. There are several bills pending in the Peruvian Congress concerning the correct definition of the crime of terrorist financing.

The UIF began operations in June 2003 and now has approximately 60 employees. In June 2007, the UIF was incorporated into the Office of the Superintendent of Banks and Insurance and a new director was appointed. As Peru's financial intelligence unit, the UIF is the government entity responsible for receiving, analyzing and disseminating suspicious transaction reports (STRs) filed by obligated entities. The entities obligated to report suspicious transactions to the UIF within 30 days include banks, financial institutions, insurance companies, stock funds and brokers, the stock and commodities exchanges, credit and debit card companies, money exchange houses, mail and courier services, travel and tourism agencies, hotels and restaurants, notaries, the customs agency, casinos, auto dealers, construction or real estate firms, notary publics, and dealers in precious stones and metals. Currently, obligated entities must hand-deliver STRs to the UIF. However, the UIF is in the transition from paper submission to automation of STR filing. Automation is supposed to be ready during the first quarter of 2009, and obligated entities will be required to implement it within three months. The UIF received 1,554 STRs in 2007 and 2,379 in 2008.

Obligated entities must also maintain reports on large cash transactions. Individual cash transactions exceeding $10,000 or transactions totaling $50,000 in one month must be maintained in internal databases for a minimum of five years and made available to the UIF upon request. Nonfinancial institutions, such as exchange houses, casinos, lotteries or others, must report individual transactions over $1,000 or monthly transactions over $5,000. Individuals or entities transporting more than $10,000 in currency or monetary instruments into or out of Peru must file reports with the customs agency, and the UIF may have access to those reports upon request. Any cash transactions that appear suspicious must be reported to the UIF and the UIF is authorized to sanction persons and entities for failure to report suspicious transactions or large cash transactions, or the transportation of currency or monetary instruments. These reporting requirements, however, are not being strictly enforced by the responsible GOP entities.

The UIF does not automatically receive currency transactions reports (CTRs) or reports on the international transportation of currency or monetary instruments. CTRs are maintained in internal registries within the obligated entities, and reports on the international transportation of currency or monetary instruments are maintained by the customs agency. If the UIF receives a STR and determines that the STR warrants further analysis, it contacts the covered entity that filed the report for additional background information-including any CTRs that may have been filed-and/or the customs agency to determine if the subject of the STR had reported the transportation of currency or monetary instruments. Some requests for reports of transactions over $10,000—such as deposits into savings accounts—are protected under the constitution by bank secrecy provisions and require an order from the Public Ministry or SUNAT, the tax authority. A period of 15 to 30 days is required to lift the bank secrecy restrictions. The Superintendent of Banks and Insurance (SBS) has the authority to request protected information under the bank secrecy provisions. However, it is not clear with the incorporation of the UIF under the SBS, whether the Superintendent may legally provide this information directly to the UIF. All other types of cash transaction reports, however, may be requested directly from the reporting institution.

Law 28.306 of 2004 mandates that obligated entities also report suspicious transactions related to terrorist financing, and expands the UIF's functions to include the ability to analyze reports related to terrorist financing. In July 2006, the GOP issued Supreme Decree 018-2006-JUS to better implement Law 28.306. The decree also introduces the specific legal framework for the supervision of obligated entities with regard to combating terrorist financing.

Law 28.306 establishes regulatory responsibilities for the UIF. Most obligated entities fall under the supervision of the SBS (banks, the insurance sector, financial institutions), the Peruvian Securities and Exchange Commission (securities, bonds), and the Ministry of Tourism (casinos). All entities that are not supervised by these three regulatory bodies, such as auto dealers, construction and real estate firms, fall under the supervision of the UIF. Under Supreme Decree 018-2006-JUS, the UIF may participate in the on-site inspections of obligated entities performed by the supervisory body. The UIF may also conduct the on-site inspections of the obligated entities that do not fall under the supervision of another regulatory body, as is the case with notaries and money exchange houses. The UIF can also request that a supervisor review an obligated entity that is not under its supervision. Supreme Decree 018-2006-JUS contains instructions for supervisors with prior UIF approval to establish which obligated entities must have a full-time compliance official (depending on each entity's size, patrimony, and other factors), and allows supervisors to exclude entities with certain characteristics from maintaining currency transaction reports.

In spite of the expanded regulatory responsibilities of the UIF, some obligated entities remain unsupervised. For instance, the SBS only regulates money remittances that are done through special fund-transfer businesses (ETFs) that do more than 680,000 soles (approximately $200,000) in transfers per year, and remittances conducted through postal or courier services are supervised by the Ministry of Transportation and Communications. As a result, informal remittance businesses, including travel agencies and small wire transfer businesses, are not supervised. There is also difficulty in regulating casinos, as roughly 60 percent of that sector is informal. An assessment of the gaming industry conducted by GOP and U.S. officials in 2004 identified alarming deficiencies in oversight and described an industry that is vulnerable to being used to launder large volumes of cash. Approximately 580 slot houses operate in Peru, with less than 65 percent or so paying taxes. Estimates indicate that less than 42 percent of the actual income earned is being reported. This billion-dollar cash industry continues to operate with little supervision.

To assist with its analytical functions, the UIF may request information from such government entities as the National Superintendence for Tax Administration, Customs, the Securities and Exchange Commission, the Public Records Office, the Public or Private Risk Information Centers, and the National Identification Registry and Vital Statistics Office, among others. However, the UIF can only share information with other agencies—including foreign entities—if there is a joint investigation underway. The UIF disseminates STRs and other reports that require further investigation or prosecution to the Public Ministry.

Within the counternarcotics section of the Public Ministry, two specialized prosecutors are responsible for dealing with money laundering cases. The UIF sent 123 suspected cases stemming from STRs to the Public Ministry for investigation in 2008. To date, there has not been a money laundering conviction in Peru. Convictions tend to be for lesser offenses such as tax evasion.

In addition to being able to request any additional information from the UIF in their investigations, the Public Ministry may also request the assistance of the Directorate of Counter-Narcotics (DINANDRO) of the Peruvian National Police. Under Law 28.306, DINANDRO and the UIF may collaborate on investigations, although each agency must go through the Public Ministry to do so. DINANDRO may provide the UIF with intelligence for the cases the UIF is analyzing, while DINANDRO provides the Public Ministry with assistance on cases that have been sent to the Public Ministry by the UIF.

The Financial Investigative Office of DINANDRO has seized numerous properties over the last several years, but few were turned over to the police to support counternarcotics efforts. While Peruvian law does provide for asset forfeiture in money laundering cases, and these funds can be used in part to finance the UIF, no clear mechanism exists to distribute seized assets among government agencies. The Garcia Administration included an asset forfeiture law in a package of organized crime legislation presented to the Peruvian Congress in July 2007. The law went into force in November 2007.

Legislative Decree No. 992, published on July 22, 2007, established the procedure for loss of dominion, which refers to the extinction of the rights and/or titles of assets derived from illicit sources, in favor of the GOP, without any compensation of any nature. Likewise, through Legislative Decree No. 635, the penal code was modified to provide more comprehensively for seizure of assets, money, earnings, or other products or proceeds of crime.

Peru is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the UN Convention for the Suppression of Financing Terrorism. The GOP is a member of the Organization of American States and participates in the Inter-American Drug Abuse Control Commission (OAS/CICAD) Money Laundering Experts Working Group. Peru also is a member of the Financial Action Task Force for South America (GAFISUD) and underwent its third GAFISUD mutual evaluation in July 2008. The UIF is a member of the Egmont Group of financial intelligence units. Although an extradition treaty between the United States and the GOP entered into force in 2003, there is no mutual legal assistance treaty or agreement between the two countries.

Although recent efforts to combat corruption and the issuance of Executive Order 25.475, which punishes terrorism-related collaboration, is a welcome step forward, the GOP nevertheless faces several notable challenges to strengthen its anti-money laundering and counterterrorist financing regime and ultimately conform to international standards. Peru should pass legislation that criminalizes terrorist financing as well as legislation that allows for administrative and judicial blocking of terrorist assets. Bank secrecy should be lifted to allow the UIF to have access to certain CTRs in a timely fashion. There are a number of bills under review in the Peruvian Congress that would lift bank secrecy provisions for the UIF in matters pertaining to money laundering and terrorist financing and the GOP should ensure their expedient passage. Peru would benefit from expanded supervision and regulation of financial institutions and designated nonfinancial businesses and professions, and the GOP should permit Peru's UIF to work directly with law enforcement agencies. Anti-corruption efforts in Peru should also be a priority. In addressing these issues, the GOP would strengthen its ability to combat money laundering and terrorist financing.

Philippines

Although the Philippines is not a regional financial center, the illegal drug trade in the Philippines has evolved into a billion dollar industry. The Philippines continues to experience an increase in foreign organized criminal activity from China, Hong Kong, and Taiwan. Insurgency groups operating in the Philippines partially fund their activities through local crime, the trafficking of narcotics and arms, and engage in money laundering through ties to organized crime. The proceeds of corrupt activities by government officials are also a source of laundered funds. Smuggling continues to be a major problem. The Federation of Philippine Industries estimates that lost government revenue from uncollected taxes on smuggled items is over $2 billion annually, including substantial losses from illegal imported fuel and automobiles. Remittances and bulk cash smuggling are also channels of money laundering. The Philippines has a large expatriate community.

The Government of the Republic of the Philippines (GOP) initially established its AML/CTF regime by passing the Anti-Money Laundering Act (AMLA) of 2001. The GOP enacted Implementing Rules

and Regulation for the AMLA in April 2002. The AMLA, as amended, criminalizes money laundering, an offense defined as a crime whereby the proceeds of an unlawful activity are transacted thereby making them appear to have originated from legitimate sources. It imposes penalties that include a term of imprisonment of up to 14 years and a fine no less than 3,000,000 pesos (approximately $63,400) but no more than twice the value of proceeds or property involved in the offense. The Act also imposes customer identification, customer due diligence, record keeping, and reporting requirements on banks, trusts, and other institutions regulated by the Bangko Sentral ng Pilipinas (BSP) or Central Bank, as well as insurance companies, and other entities under the supervision or regulation of the Insurance Commission, securities dealers, foreign exchange dealers, money remitters, and dealers in valuable objects or cash substitutes regulated by the Securities and Exchange Commission (SEC).

The GOP amended the AMLA in 2003 to correct certain inadequacies identified by the Financial Action Task force. The amendments included lowering the threshold amount for covered transactions (cash or other cash equivalent monetary instrument) from 4,000,000 pesos to 500,000 pesos (approximately $85,000 to $10,600); expanded financial institution reporting requirements to include the reporting of suspicious transactions regardless of amount; authorized the Central Bank to examine any particular deposit or investment with any bank or nonbank financial institution in the course of a period or special examination (in accordance with the rules of examination of the Central Bank); ensure institutional compliance with the Anti-Money Laundering Act; and deleted the prohibitions against the Anti-Money Laundering Council's examining particular deposits or investments opened or created before the Act.

The original AMLA established the Anti-Money Laundering Council (AMLC) as the country's financial intelligence unit (FIU). The Council is composed of the Governor of the Central Bank, the Commissioner of Insurance Commission, and the Chairman of the Securities and Exchange Commission. By law, the AMLC is an independent agency responsible for receiving, maintaining, analyzing, evaluating covered and suspicious transactions and investigating reports for possible criminal activity. It provides advice and assistance to relevant authorities and issued relevant publications. The AMLC completed the first phase of its information technology upgrades in 2004. This allowed AMLC to electronically receive, store and search "covered transaction reports" (CTRs) filed by regulated institutions. By the end of 2008, the AMLC had received more than 17,915 suspicious transactions reports (STRs), and 133,367,756 CTRs. The AMLC is a member of the Egmont Group.

On February 28, 2007, the AMLC entered into a Memorandum of Understanding with the Central Bank setting forth the procedures for improved information exchange, compliance and enforcement policies.

AMLC's role goes beyond traditional FIU responsibilities and includes the investigation and assisting the Office of the Solicitor General in the handling of civil forfeiture cases. AMLC has the ability to institute civil actions for forfeiture of monetary instruments or property involved in any unlawful activity defined in the AMLA, as amended. No prior criminal charge or conviction for an unlawful activity or money laundering offense is necessary for a commencement of an action or resolution of a petition for civil forfeiture. To freeze assets allegedly connected to money laundering, the AMLC must establish probable cause that the funds relate to an unlawful activity enumerated in the Act. The Court of Appeals then may freeze a bank account for 20 days. Through the end of 2007, funds amounting to almost 1.4 billion Philippine pesos (approximately $30 million) have been frozen by the AMLC, including funds frozen at the request of the UN Security Council, the United States, and other foreign governments. It has also received 66 official requests for anti-terrorism action, many concerning groups on the UNSCR 1267 Sanction Committee's consolidated list.

The AMLC is required to secure a court order to examine bank records related to the unlawful activities enumerated in the AMLA, as amended, except in instances where the unlawful activity is a serious offense such as kidnapping for ransom, drugs and terrorism-related activities.

A Supreme Court of the Philippine's decision to suspend certain inquiries into suspicious transactions will have significant adverse consequences for Philippines law enforcement in extending international cooperation to its partners. As it stands, the AMLC will have to prematurely divulge to account holders the fact of the investigation and the basis for inspecting the bank records. This will result in providing criminals both with an advance notice of proceedings and progress of the investigation, and as well as the identities of persons cooperating with law enforcement. Aside from jeopardizing the investigation by tipping them off, it will also afford the criminal an opportunity to do shelter assets making the tracing of the funds virtually impossible.

The Philippines has no comprehensive legislation pertaining to civil and criminal forfeiture. Various government authorities, including the Bureau of Customs and the Philippine National Police, have the ability to temporarily seize property obtained in connection with criminal activity. Money and property must be included in the indictment, however, to permit forfeiture.

In December 2005, the Supreme Court issued the Rule of Procedure in Cases of Civil Forfeiture, Asset Preservation and Freezing of Monetary Instrument, Property, or Proceeds Representing, Involving, or Relating to an Unlawful Activity or Money Laundering Offense under the AMLA, as amended. The Rule also contains direction to the AMLC and the Court of Appeals on the issuance of freeze orders for assets under investigation, eliminating confusion arising from the amendment to the AMLA in 2003.

As of December 2007, there have been 107 money laundering, civil forfeiture, and related cases in the Philippines court system that involved AMLC investigations or prosecutions, including 37 for money laundering, 20 for civil forfeiture, and the rest pertaining to freeze orders and bank inquiries. The Philippines had its first conviction for a money laundering offense in early 2006.

Under the AMLA, as amended, covered institutions and their officers and employees, shall not be deemed to have violated Republic Act No. 1405, as amended (Law on Secrecy of Bank Deposits); Republic Act No. 6426, as amended; Republic Act No. 8791 and other similar laws, when reporting covered or suspicious transactions. Further, no administrative, criminal or civil proceedings shall lie against any person for having made a covered or suspicious transaction report in the regular performance of his duties and in good faith.

Covered institutions must maintain and store records of transactions for a period of five years from the dates of transactions. With respect to closed accounts, the records on customer identification, account files and business correspondence shall be preserved and safely stored for at least five years from the dates when they were closed.

The AMLC and the supervising authorities such as the Central Bank, Securities and Exchange Commission and the Insurance Commission monitor compliance with the AMLA provisions by banks and other financial institutions identified as covered institutions. They have mechanisms in place to ensure that the financial community is adhering to reporting and other AMLA requirements. To enhance on-going monitoring and reporting of covered and possible suspicious transactions, the BSP issued Circular No. 495 dated 20 September 2005 which requires all universal and commercial banks to adopt an electronic money laundering transaction monitoring system which, at a minimum, shall detect and raise to the bank's attention, transactions and/or accounts that qualify either as "covered transactions" or "suspicious transactions" as defined under Sections 3(b) and 3(b-1), respectively, of the AMLA, as amended.

The AMLC continues to work to bring the numerous foreign exchange offices in the country under its purview. The BSP issued Circular No. 471 dated 24 January 2005 to bring the registration and operations of foreign exchange dealers and remittance agents under the jurisdiction and authority of the BSP and to subject them to the AMLA, as amended. To obtain a license, one of the requirements is that dealers must attend an AML/CTF training course conducted by the AMLC. As of the beginning of 2008, only 4,144 of the estimated 15,000 exchange dealers and remittance agents have registered. There are still several sectors operating outside of AMLC control.

Although the AMLA specifically covers exchange houses, insurance companies, and securities brokers, it does not cover designated nonfinancial business and professions except trust companies. The AMLC requires automobile dealers and vendors of construction equipment, which are emerging money laundering methodologies, to report suspicious transactions to the AMLC.

On 15 March 2007 the Central Bank issued Circular No. 564 establishing guidelines governing the acceptance of valid identification cards including the AMLA's "two-ID requirement" for conducting financial transactions with banks and nonbank institutions. This was later amended by Circular No. 608 issued by the BSP on 20 June 2008, relaxing the customer identification requirement to be imposed by banks and other institutions under BSP supervision or regulation. Currently, one identification card issued by an official authority as defined in BSP Circular No. 608, is sufficient.

Casinos are regulated by the Philippine Amusement and Gaming Corporation (PAGCOR) pursuant to P.D. No. 1869. The Cagayan Economic Zone Authority (CEZA) is likewise granted by Republic Act No. 7922 the authority to license casinos. Both PAGCOR and CEZA are under the supervision of the Office of the President (OP). The OP, in its letter dated 10 December 2007, advised the AMLC that a legislative amendment is required as the law did not define casinos as covered institutions.

There is an increasing recognition that the 15 casinos nationwide offer abundant opportunity for money laundering, especially with many of these casinos catering to international clientele arriving by charter flights from around Asia. Several of these gambling facilities are located near small provincial international airports that may have less rigid enforcement procedures and standards for cash smuggling. At present, there are no offshore casinos in the Philippines, though the country is a growing location for Internet gaming sites that target overseas audiences in the region. PAGCOR has agreed to voluntarily submit reports on suspicious activities of casino operators or its patrons.

As of March 2008, there are 76,512 nonstock, nonprofit organizations (NPOs) registered with the Securities and Exchange Commission (SEC). These NPOs do not fall under the requirements of the AMLA, as amended. All nonstock and nonprofit organizations registered with the Securities and Exchange Commission (SEC) are required to annually submit General information Sheets and Audited Financial Statements. Because of their ability to circumvent the usual documentation and reporting requirements imposed on banks for financial transfers, NGOs could be used as conduits for terrorist financing without detection. The AMLC is aware of the problem and is working with the SEC to bring charitable and not-for-profit entities under regulations for covered institutions. To promote transparency, SEC Circular 8 issued in June 2006 revised regulations on the registrations, operations, and audit of foundations. In July 2007, the AMLC initiated the organization of a Technical Working Group (TWG) on the Non-Profit Organization, which conducted a survey on the NPO sector. There are regular meetings among NPOs providing for a venue to discuss measures for the effective prevention of money laundering and terrorist financing within the NPO environment.

There are seven offshore banking units (OBUs), which account for less than three percent (3 percent) of total banking system assets in the country. The Central Bank regulates onshore banking and exercises regulatory supervision over OBUs, and requires OBUs to meet reporting provisions and other banking rules and regulations. In addition to registering with the SEC, financial institutions must obtain certification to operate from the Central Bank subject to relatively stringent standards that make it difficult to establish shell companies in financial services of this nature. For example, a financial

institution operating an OBU must be physically present in the Philippines. Anonymous directors and trustees are not allowed.

Despite the efforts of authorities to publicize regulations and enforce penalties, cash smuggling remains a major concern for the Philippines. Although there is no limit on the amount of foreign currency that an individual or entity can bring or take out of the country, any amount in excess of the equivalent of $10,000 of cash or negotiable instruments must be declared upon arrival or departure. However, based on the actual amount of foreign currency exchanged and expended, authorities realize there is systematic abuse of the currency declaration requirements and a large amount of unreported cash entering the Philippines.

The problem of cash smuggling is exacerbated by the large volume of foreign currency remitted to the Philippines by Overseas Filipino Workers (OFW). In 2007, the amount of remitted funds exceeded $14 billion or approximately 11 percent of the GDP. The Central Bank estimates that an additional $2-3 billion is remitted outside the formal banking system. Most of these funds are brought in person by OFWs or by designated individuals on their return home and not through an alternative remittance system such as hawala or an unofficial “door-to-door” delivery system. Since most of these funds enter the country in smaller quantities than $10,000, there is no declaration requirement and the amounts are difficult to calculate. The Philippines encouraged banks to set up offices in remitting countries and facilities for fund remittances, especially in the United States, to help reduce the expense of remitting funds. OFWs also use informal value transfer systems.

The Philippines is a member of the Asia/Pacific Group on Money Laundering (APG). The APG conducted a comprehensive peer review of AMLC in September 2008 and subsequently provided 45-pages of recommendations for improvement. Prominent APG concerns include the exclusion of PAGCOR from the scope of current anti-money laundering legislation, and 2008 court rulings that expanded the scope of bank privacy laws to an extent that inhibits investigations of fraud and corruption. The Philippine legislature is now considering an amendment to the Anti-Money Laundering Act of 2001 to address these issues.

A mutual legal assistance treaty between the Philippines and the United States has been in force since 1996. The Philippines is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption and the UN Convention for the Suppression of the Financing of Terrorism. The Philippines is listed 141 out of 180 countries surveyed by Transparency International’s 2008 International Corruption Perception Index.

The Anti-Money Laundering Council must obtain a court order to freeze assets of terrorists and terrorist organizations placed on the UN 1267 Sanctions Committee’s consolidated list and the list of Specially Designated Global Terrorists Designated by the United Sates pursuant to E.O. 13224 and actions by other foreign governments. In 2007, the GOP enacted an anti-terrorism law that defines and criminalizes terrorism. The Human Security Act which went into effect on July 15, 2007 criminalizes terrorism and conspiracy to commit terrorism; penalizes an offender on the basis of participation; empowers Philippine law enforcement to use special investigative techniques; allows inquiries into bank accounts; authorizes freezes and forfeitures of terrorist related funds and assets; and creates an Anti-Terrorism Council comprised of cabinet members and support agencies.

While there is no crime of terrorist financing a person who finances the commission of terrorism may be prosecuted, not as a financier of terrorism but as a terrorist either as a principal by inducement pursuant to Article 17 of the Revised Penal Code or as an accomplice pursuant to Section 5 of the Human Security Act

The Financial Action Task Force removed the Government of the Republic of the Philippines from its list of Non-Cooperative Countries and Territories in 2005 due to the progress the Government of the Philippines had made in remedying the deficiencies that resulted in its being placed on the list in 2001.

Since 2005, the Government of the Philippines (GOP) has continued to make progress enhancing and implementing its amended anti-money laundering regime. The Central Bank should be empowered to levy administrative penalties against covered entities in the financial community that do not comply with reporting requirements. Accountants should be required to report CTRs and STRs. Casinos should be fully regulated and supervised for AML/CTF procedures and required to file STRs. To become a more effective FIU, the AMLC should expeditiously revise its structure and separate its analysts and investigators into separate divisions. The GOP should enact comprehensive legislation regarding freezing and forfeiture of assets that would empower the AMLC to issue administrative freezing orders to avoid funds being withdrawn before a court order is issued. The GOP does have a civil asset forfeiture regime; however, the asset forfeiture fund should allow law enforcement agencies to draw on the fund to augment their budgets for investigative purposes. Such a fund would benefit the AMLC and enable it to purchase needed equipment. The AMLC should separate its analytical and investigative responsibilities and establish a separate investigative division that would focus its attention on dismantling money laundering and terrorist financing operations. In addition, law enforcement should be able to scrutinize financial records as an investigative measure on an ex parte basis when notice to the account holder might prejudice the ability of the government to successfully prosecute the money laundering or forfeiture case, including enabling a suspected criminal to take action to secrete or transfer assets.

Poland

Poland lies directly along one of the main routes between the former Soviet Union republics and Western Europe used by narcotics-traffickers and organized crime groups. According to Polish Government estimates, narcotics trafficking, organized crime activity, auto theft, smuggling, extortion, counterfeiting, burglary, and other crimes generate criminal proceeds in the range of $3,000,000,000 to $5,000,000,000 each year. According to the Government of Poland (GOP), fuel smuggling, by which local companies and organized crime groups seek to avoid excise taxes by forging gasoline delivery documents, is a major source of laundered proceeds. With regard to economic crime, the largest volume of illegal income is connected with lost customs duties and taxes. Money laundering through trade in scrap metal and recyclable material is a growing trend. It is also believed that some money laundered in Poland originates in Russia or other countries of the former Soviet Union. The GOP estimates the unregistered or gray economy, used primarily for tax evasion, may be as high as 13 percent of Poland's $620,000,000,000 gross domestic product (GDP). The GOP believes the black economy comprises only one percent of GDP.

Reportedly, some of Poland's banks serve as transit points for the transfer of criminal proceeds. As of June 2007, 51 commercial banks and 584 "cooperative banks" primarily serving the rural and agricultural community were licensed to operate. The GOP considers the nation's banks, insurance companies, brokerage houses, and casinos to be important venues of money laundering. The Finance Ministry maintains the effectiveness of actions against money laundering involving transfer of money to so-called tax havens is limited. Poland's entry into the European Union (EU) in May 2004 and into the Schengen zone in December 2007 has increased its ability to control its eastern borders, thereby allowing Poland to become more effective in its efforts to combat all types of crime, including narcotics trafficking and organized crime.

In 2006, the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), a Financial Action Task Force (FATF)-style regional body, conducted its third round mutual evaluation of Poland. The report shows Poland to be noncompliant with international standards regarding customer due diligence (CDD). Polish legislation still lacks many important provisions regarding customer identification procedures when starting a business relationship, verification of identification data, and ongoing or enhanced CDD. There is no prohibition on the opening of an account when satisfactory CDD cannot be

completed. Nor is there a requirement to terminate a customer relationship when the financial institution cannot complete CDD.

As of June 2008, the European Commission (EC) was pursuing an infringement action against Poland for failing to adopt and implement the Third EU Anti-Money Laundering Directive into national law by the mandated deadline. In January 2009, the EC made the decision to refer Poland to the European Court of Justice over its non-implementation of this Directive, which requires members to update their AML regimes to comport with the most up-to-date standards, particularly with regard to regulation and terrorism financing.

The Criminal Code criminalizes money laundering for all serious crimes. Article 299 of the Criminal Code addresses self-laundering and criminalizes tipping off. The Polish Code of Criminal Procedure, Article 237, allows for certain special investigative measures (SIM). Although money laundering investigations are not specifically discussed in relation to SIM, the organized crime provisions might apply in some cases. Although Poland's definition of money laundering is largely compliant with international standards, it still lacks some important components. For instance, some of the legislative provisions need further clarification regarding certain elements (conversion, acquisition, possession, and use) of money laundering. In addition, more emphasis is needed on third party laundering and clarifying the evidence required to establish the underlying predicate criminal offense.

Poland's anti-money laundering (AML) regime begins in November 1992, when the President of the National Bank of Poland issues an order instructing banks how to deal with money entering the financial system through illegal sources. The August 1997 Banking Act and 1998 Resolution of the Banking Supervisory Commission add customer identification requirements and institute a threshold reporting requirement.

The November 2000 Act on Counteracting Introduction into Financial Circulation of Property Values Derived from Illegal or Undisclosed Sources and on Counteracting the Financing of Terrorism, as amended, further improves Poland's ability to combat money laundering. This law, which the GOP has updated to improve its operational effectiveness, increases penalties for money laundering and contains safe harbor provisions that exempt financial institution employees from normal restrictions on the disclosure of confidential banking information. Parliament further amended the law to broaden the definition of money laundering to include assets originating from illegal or undisclosed sources. Several additional amendments to the 2000 money laundering law expand the scope of institutions subject to identity verification, record keeping, and suspicious transaction reporting requirements. Entities subject to the reporting requirements include banks, the National Depository for Securities, post offices, auction houses, antique shops, brokerages, casinos, insurance companies, investment and pension funds, leasing firms, private currency exchange offices, real estate agencies, notaries public, lawyers, legal counselors, auditors, and charities, as well as the National Bank of Poland in its functions of selling numismatic items, purchasing gold, and exchanging damaged banknotes.

The law requires casinos to report the purchase of chips worth 1,000 euros (approximately $1,350) or more. In addition to requiring that obligated entities notify the financial intelligence unit (FIU) of all transactions exceeding 15,000 euros (approximately $20,250), covered institutions also must file suspicious transaction reports (STRs), regardless of the size of the transaction. Polish law also requires financial institutions to put internal AML procedures into effect, a process overseen by the FIU.

The Polish Bar mounted a challenge against certain provisions of the legislation, and submitted a motion to the Constitutional Tribunal to determine the consistency of various regulations with ten articles of the Polish Constitution. On July 2, 2007, the Constitutional Tribunal issued a ruling that lawyers are allowed to refrain from notifying the relevant authorities of suspicious transactions when they provide legal assistance to and determine the legal status of a client.

The "Act on Counteracting Money Laundering and Terrorism Financing" underwent numerous revisions in 2008. The draft legislation has been submitted to Parliament, and it is expected to become law in early 2009. The legislation will enhance existing AML legislation.

As of June 15, 2007, travelers entering Poland from a non-EU country or traveling to a non-EU country with 10,000 euros (approximately $13,500) or more must declare their cash or monetary instruments in writing. Poland's customs law requires travelers to complete and present a customs and currency declaration if they are transporting more than the threshold amount upon entry. In December 2007, the new Schengen countries, including Poland, were enveloped within EU borders. Land border controls between EU member states disappeared on December 20, 2007, and airport controls in March 2008.

The 2000 AML law provides for the creation of a FIU, the Department of Financial Information (DFI), within the Ministry of Finance, to collect and analyze large cash and suspicious transactions and perform regulatory work. The vast majority of required notifications to the DFI come through the electronic reporting system. Only some small institutions lacking the equipment to use the electronic system submit notifications on paper. Although the new system is an important tool for Poland's AML regime, the efficient processing and analysis of the large number of reports sent to the DFI is a challenge for the understaffed FIU. To help improve the FIU's efficiency, the DFI continues to work on a specialized IT program that will support complex data analysis and improve the FIU's ability to handle the increasing number of reports it receives.

In 2007, the DFI received a total of 18,115 STRs. The number of STRs submitted by cooperative entities rose to 648, an increase of 22 percent from the previous year; 69 percent of these came from the Agricultural Property Agency and from fiscal offices. Altogether, the DFI analyzed 10,776 STRs.

As a result of its analysis, in 2007, the DFI initiated 1,358 analytical proceedings connected with suspicious financial transactions. The proceedings generally concerned illegal or fictitious trade in fuels and/or scrap metal (165), trade in funds originating from fraud and/or obtained under false pretenses (122), trade in funds originating from unauthorized access to bank accounts (14), transactions by nonresidents (46), and transfers of money related to fictitious invoicing, real-estate funds, and securities. The DFI demanded the suspension of just one transaction for PLN 230,000 (approximately $79,000) and the freezing of 97 accounts worth an estimated PLN 30 million (approximately $10,300,000). The DFI also froze 58 accounts on its own initiative worth an estimated PLN 7.1 million (approximately $2,400,000).

Altogether, the DFI submitted 190 notifications to the Public Prosecutor's Office under Article 299 of the Criminal Code, representing an estimated PLN 775 million (approximately $337,000,000) in transactions. Of these, 116 resulted in initial investigative proceedings. In 2007, 176 of the 296 money laundering cases initiated by the Public Prosecutor's Office were based on information received from the DFI. The cases resulted in 82 indictments against 288 persons. The courts returned 36 guilty verdicts and convicted 55 individuals on charges of money laundering. The total value of all seized property was approximately PLN 40.5 million (approximately $14,000,000).

In addition to the Prosecutor's Office, the DFI also cooperates with several domestic law enforcement agencies, including the Central Investigative Bureau (CBS), a police unit; the Internal Security Agency (ABW), which investigates the most serious money laundering cases; and the Central Anti-Corruption Office (CBA). Coordination and information exchange between the DFI and law enforcement entities has improved, especially with regard to the suspicious transaction information the DFI forwards to the National Prosecutor's Office. The DFI and the National Prosecutor's Office have signed a cooperation agreement calling for the creation of a computer-based system to facilitate information exchange between the two institutions. Work on the development of this new system is currently underway.

In 2006, DFI conducted an assessment of the effectiveness of Poland's AML reporting system. According to the DFI's 2006 annual report, the analysis identified three main threats to efficiency of the system: disproportionate reporting among Poland's 16 provinces (three provinces had extremely high reporting rates); delays in prosecutorial handling of DFI notifications; and inadequate use of the DFI by the full range of domestic agencies in Poland (76 percent of all queries to the DFI were from the Prosecutor's office).

The DFI now conducts all training online via e-learning, which is available to all obligated institutions and cooperative entities. In 2007, 2,074 representatives from obligated institutions and 116 employees of cooperative institutions participated in the electronic learning course, a two-week course consisting of nine lessons. The course finishes with an online test and certificate of completion.

The DFI exchanges information with its foreign counterparts. The United States, United Kingdom, Ukraine, Russia, Cyprus, and Belgium are among its most active information-sharing partners. In 2007, DFI sent official information requests to foreign FIUs on 175 cases concerning 308 national and foreign entities suspected of money laundering. Foreign FIUs sent 111 information requests concerning 460 national and foreign entities to the DFI.

The DFI has the authority to put a suspicious transaction on hold for 48 hours. The Public Prosecutor then has the right to suspend the transaction for an additional three months, pending a court decision. Article 45 of the criminal code reverses the burden of proof so that an alleged perpetrator must prove his assets have a legal source; otherwise, the assets are presumed to be related to the crime and the government can seize them. Both the Ministry of Justice and the DFI reportedly desire more aggressive asset forfeiture regulations. However, lingering political sensitivities reportedly hamper approval of stringent asset seizure laws.

Poland is not compliant with international standards with regard to the criminalization of terrorist financing. Poland has not yet criminalized terrorist financing as is required by UNSCR 1373, arguing that all possible terrorist activities are already illegal and serve as predicate offenses for money laundering and terrorist financing investigations. Under current provisions, it is unclear how Poland could directly prosecute the funding of a terrorist or terrorist organization; it is only addressed through conspiracy or aiding and abetting terrorism. No terrorist financing prosecutions have yet been undertaken or cases brought before the court. The Ministry of Justice prepared a draft of amendments to the criminal code that would criminalize terrorist financing as well as elements of all terrorism-related activity, but withdrew the draft in 2007, before it had been approved by the Council of Ministers.

The GOP has created an office of counterterrorist operations within the National Police, which coordinates and supervises regional counterterrorism units and trains local police in counterterrorism measures. In 2008, the Polish Ministry of Interior and Administration created a national Anti-Terrorist Center (CAT), which became operational in October 2008. CAT is a 20-person team, responsible for coordinating efforts of the police, the army, and the Civil Security Services. They are to secure Poland's borders and prevent terrorism in the country. The CAT has the authority to immediately mobilize police forces and the army. Poland has also created its own terrorist watch list of entities suspected of involvement in terrorist financing. The list contains the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list, the names of Specially Designated Global Terrorists designated by the U.S. pursuant to Executive Order 13224, and the names designated by the EU under its relevant authorities. All obligated institutions must verify their customers are not included on the watch list. In the event a covered institution discovers a possible terrorist link, the DFI has the right to suspend suspicious transactions and accounts. In 2007, the DFI worked on seven terrorist financing cases involving 77 subjects. Upon completion of its analysis, the DFI forwarded 14 reports to the ABW for further analysis. The cases related to

transactions involving large amounts of cash being sent to Poland as well as numerous noncash transfers involving terrorist groups or parties from a country supporting terrorism.

A Mutual Legal Assistance Treaty (MLAT) between the United States and Poland came into force in 1999. In addition, Poland has signed bilateral MLATs with Sweden, Finland, Ukraine, Lithuania, Latvia, Estonia, Germany, Greece, and Hungary. Polish law requires the DFI to have memoranda of understanding (MOUs) with other international competent authorities before it can participate in information exchanges. The DFI has been diligent in executing MOUs with its counterparts in other countries, including two in 2007 (Albania and Montenegro) and one in 2008 (Mexico), for a total of 39 MOUs. The MOU between the Polish FIU and the U.S. FIU was signed in fall 2003.

Poland is a member of MONEYVAL. The DFI is a member of the Egmont Group and is enrolled in FIU.NET, the EU-sponsored information exchange network for FIUs. All information exchanged between the DFI and its counterparts in other EU states takes place via FIU.NET or the Egmont Secure Web system. Poland is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption.

Over the past several years, the Government of Poland has worked to implement a comprehensive AML regime that meets international standards. However, work remains, as Poland's AML regime remains noncompliant with various FATF standards. Most significantly, Poland must criminalize terrorist financing. The GOP should review and clarify its definition of money laundering to bring it in line with international standards. Poland must also strengthen AML regulations pertaining to customer due diligence obligations, DNFBPs, nonprofit organizations, politically exposed persons, cross-border correspondent banking, and suspicious transaction reporting as it pertains to terrorist financing. Poland should ensure promulgating regulations for compliance with the Third Money Laundering Directive are fully effective. The GOP should promote additional capacity building in the private sector and continue to improve communication and coordination between the DFI and relevant law enforcement agencies. The Code of Criminal Procedure also should be amended to specifically allow the use of special investigative measures in money laundering investigations, which would assist law enforcement in its efforts to attain a better record of prosecutions and convictions.

Portugal

Portugal is an entry point for narcotics transiting into Europe, and officials of the Government of Portugal (GOP) indicate the majority of money laundered in Portugal is narcotics-related. Currency exchanges, wire transfers, and real estate purchases are used for laundering criminal proceeds.

Portugal has a comprehensive anti-money laundering and counterterrorist financing (AML/CTF) regime that criminalizes the laundering of proceeds of serious offenses, including terrorism, arms trafficking, kidnapping, and corruption. Article 11 of Law 59/2007, dated September 4, 2007, defines money laundering, expands the list of crimes related to money laundering, and makes legal entities criminally accountable. In April 2008, Portugal enacted Law 25/2008, which made a series of enhancements to the AML/CTF system.

The three principal regulatory agencies for supervision of the financial sector in Portugal are the BoP, the Portuguese Insurance Institute, and the Portuguese Securities Market Commission. Law 11/2004 broadened the GOP's AML regime. Law 11/2004 mandates suspicious transaction reporting by credit institutions, investment companies, life insurance companies, traders in high-value goods (e.g., precious stones, aircraft), and numerous other entities. Portugal employs an all-crimes approach to the predicate offense. "Tipping off" is prohibited and obliged entities making disclosures in good faith enjoy liability protection. Law 49/2008 consolidated criminal investigative responsibilities for money

laundering and terrorist finance under the Judicial Police's authority to facilitate more centralized investigations.

If an obliged entity has knowledge of a transaction likely to be related to a money laundering offense, it must inform the GOP, which may order the entity not to complete the transaction. If stopping the transaction is impossible or potentially detrimental to law enforcement efforts, the government also may allow the transaction to proceed but require the entity to provide complete transaction details.

All financial institutions must identify their customers, maintain records for a minimum of ten years, and demand written proof from customers regarding the origins and beneficiaries of transactions that exceed 12,500 euros (approximately $16,533). Nonfinancial sectors such as casinos, property dealers, lotteries and dealers in high-value assets, must also identify customers engaging in large transactions, maintain records, and report suspicious activities. Law 25/2008 of April 2008 included new enhanced due diligence requirements for entities dealing with politically exposed persons (PEPs).

Decree-Law 295/2003 of November 2003 sets out reporting requirements for the cross-border transportation of cash, nonmanufactured gold, and certain negotiable financial instruments, such as travelers' checks. When a person travels across the Portuguese border with more than 12,500 euros worth of such assets, the traveler must declare the assets to Portuguese customs officials. With Decree-Law 61/2007, Portugal requires all individuals to declare currency valued at 10,000 euros (approximately $14,600) or greater when entering or exiting Portugal from outside the European Community. The law also requires that authorities gather and exchange information at the national and international levels.

The 2006 Financial Action Task Force (FATF) mutual evaluation report (MER) noted that Portugal's mechanism for determining beneficial ownership does not fully comply with FATF standards. The National Registry of Legal Persons does not include all information to reveal the beneficial owners of legal persons. Instructions and regulatory standards set forth by the Bank of Portugal (BoP) and the Portuguese Insurance Institute (ISP) house the requirements for obliged entities to identify beneficial owners, as opposed to being stipulated by law. The Securities Market Commission (CMVM) regulations also do not explicitly comply with requirements regarding the identification of the beneficial owners of legal persons.

The November 2003 law also revised and tightened the legal framework for gold and foreign currency exchange transactions, subjecting them to a reporting requirement for transactions exceeding 12,500 Euros (approximately $16,533). Beyond the requirements to report large transactions, foreign exchange bureaus have no special requirements to report suspicious transactions. The law does, however, give the GOP the authority to investigate suspicious transactions without notifying targets of the investigation.

Rules require companies to have at least one bank account and, for companies with more than 20 employees, to conduct their business through bank transfers, checks, and direct debits rather than cash. Tax authorities may lift secrecy rules without authorization from the target of an investigation. The concept behind these rules is mainly to help the GOP investigate tax evasion, but authorities may use them to facilitate enforcement of other financial crimes as well.

The Portuguese Securities Market Commission issued Regulation 7/2005, entering into force on January 1, 2006, requiring financial intermediaries to submit detailed annual Control and Supervision Reports to the Commission by June 30 of the following year. Regulation 2/2006 entered into force on May 26, 2006. These Regulations amended and updated Regulation 12/2000 on Financial Intermediaries.

The Gambling Inspectorate General, the Economic Activities Inspectorate General, the Registries and Notaries General Directorate, the National Association for Certified Public Accountants and the Association for Assistant Accountants, the Bar Association, and the Chamber of Solicitors monitor

and enforce the reporting requirements of designated nonfinancial businesses and professions, including casinos, realtors, dealers in precious metals and stones, accountants, notaries, statutory auditors, registry officials, attorneys and solicitors. Although Internet gaming is widely available, accessing Internet gaming sites is illegal in Portugal and there are no known casinos or gaming websites whose Internet service providers are headquartered in Portugal.

Decree-Law 304/2002 of December 13, 2002, established Portugal's financial intelligence unit (FIU), known as Unidade de Informação Financeira (UIF), or the Financial Information Unit. It operates independently as a department of the Portuguese Judicial Police (Polícia Judiciária). The 28 persons comprising UIF are responsible for gathering, centralizing, processing, and publishing information pertaining to investigations of money laundering, tax crimes, and with Law 25/2008, terrorist financing. It also facilitates cooperation and coordination with other judicial and supervising authorities but.has no regulatory authority in the area of AML/CTF issues. In 2007, the UIF received 724 STRs. The FIU also received over 15,000 other reports, primarily from the General Inspectorate for Gaming. At the international level, the UIF coordinates with other FIUs.

Between 2002 and 2005, sixteen persons were convicted of money laundering receiving penalties ranging from one year to eight and one-half years' imprisonment. During 2007, Portuguese authorities pursued 95 investigations and 25 prosecutions, and obtained four convictions for money laundering. During the first six months of 2008, Portugal saw 46 investigations, 26 prosecutions, and 14 convictions for money laundering.

Portuguese laws provide for the confiscation of assets connected to money laundering and authorize the Judicial Police to trace illicitly obtained assets (including those passing through casinos and lotteries), even if the predicate offense occurs outside of Portugal. Police may request files of individuals under investigation and, with a court order, can obtain and use audio and videotape as evidence in court. The law allows the Public Prosecutor to request a lien on the assets of individuals under prosecution in order to facilitate asset seizures related to narcotics and weapons trafficking, terrorism, and money laundering. Between January and September of 2007, the UIF seized or confiscated approximately 32.4 million euros (approximately U.S. $47.3 million).

Law 5/2002 partially shifted the burden of proof in cases of criminal asset forfeiture from the government to the defendant; an individual must prove that he or she did not obtain the assets in question as a result of criminal activity. According to the 2006 FATF MER, however, a defendant must show a legitimate source of the assets only after conviction. The law defines criminal assets as those owned by an individual at the time of indictment and thereafter. The law also presumes that assets transferred by an individual to a third party within the previous five years still belong to the individual in question, unless proven otherwise. In drug-related cases, Portugal has comprehensive legal procedures that enable it to cooperate with foreign jurisdictions and share seized assets.

Law 52/2003 defines terrorist acts and organizations and criminalizes the transfer of funds related to the commission of terrorist acts. It also addresses the criminal liability of legal persons for terrorism financing. However, the legislation does not extend customer due diligence requirements to suspected association with terrorism financing. And while the broadly worded law covers both illicit and licit funds that support a terrorist act or organization, it does not extend coverage to the provision of funds to an individual terrorist. Portugal has created a Terrorist Financing Task Force that includes the Ministries of Finance and Justice, the Judicial Police, the Security and Intelligence Service, the Bank of Portugal, and the Portuguese Insurance Institution. Names of individuals and entities included on the United Nations Security Council Resolution 1267 Committee's consolidated list, or that the United States or EU have linked to terrorism, are passed to private sector entities through the BoP, the Stock Exchange Commission, and the Portuguese Insurance Institution. In practice, however, the actual seizure of assets would only occur once the EU's clearinghouse process agrees to the EU-wide seizure of assets of terrorists and terrorist-linked groups. Although Portugal does not have an administrative

procedure to freeze assets independently of the relevant EU directive, judicial procedure exists for the Public Prosecutor to open a special inquiry and to freeze assets at the request of a foreign country. To date, no significant assets have been identified or seized. The FATF MER refers to "deficiencies in scope and time" relating to the freezing of terrorism-related funds.

The Madeira International Business Center (MIBC) has a free trade zone, an international shipping register, offshore banking, trusts, holding companies, stock corporations, and private limited companies. The latter two business groups, similar to international business corporations, account for approximately 6,500 companies registered in Madeira. All entities established in the MIBC will remain tax exempt until 2011. Twenty-seven offshore banks are currently licensed to operate within the MIBC. The Madeira Development Company supervises offshore banks. There is no indication that the MIBC has been used for money laundering or terrorist financing.

Companies can also take advantage of Portugal's double taxation agreements. Decree-Law 10/94 permits existing banks and insurance companies to establish offshore branches. Companies submit applications to the BoP for notification or authorization. The law allows establishment of "external branches" that conduct operations exclusively with nonresidents or other Madeiran offshore entities, and "international branches" that conduct both offshore and domestic business. Although Madeira has some local autonomy, Portuguese and EU legislative rules regulate its offshore sector, and the competent oversight authorities supervise it. Exchange of information agreements contained in double taxation treaties allow for the disclosure of information relating to narcotics or weapons trafficking. Laws prohibit bearer shares.

Portugal is a member of the FATF. Portugal is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. Portugal's FIU is a member of the Egmont Group. According to the FATF MER, Portugal has undertaken many mutual legal assistance obligations, especially with regard to identification, seizure and confiscation of assets.

The Government of Portugal has implemented a comprehensive and effective regime to combat money laundering and spent the last decade honing its ability to investigate and prosecute money laundering cases, and extending its reach to terrorist financing. Legislative measures have consolidated the anti-money laundering legal framework, imposing on financial and nonfinancial institutions obligations to prevent the use of the financial system for the purpose of money laundering. The GOP continued to implement these measures in 2008 to effectively combat money laundering and terrorist financing. The GOP should work to correct identified deficiencies in its asset freezing and forfeiture regime, improve its mechanisms to determine beneficial owners, and amend the terrorism financing law to make it applicable to individuals.

Qatar

Supported by energy-driven double-digit economic growth in recent years, Qatar is an increasingly important banking and financial services center in the Gulf. Despite the growth of the banking sector and increasing options for financial services, Qatar still has a cash-intensive economy. Traditionally, Qatar has had a low rate of general and financial crime, although crime rates have increased in recent years and the financial sector's expansion could make it an increasingly appealing target for criminals. Moreover, there are several trends which make Qatar increasingly vulnerable to money laundering including: the large number of expatriate laborers who send remittances to their home countries; the growth in trade; liberalization and growth in the real estate sector; increase in the price of precious metals; uneven corporate oversight; and, an apparent lack of financial crimes enforcement.

Qatar is a member of the Middle East and North Africa Financial Action Task Force (MENA-FATF). In mid-2008, the International Monetary Fund (IMF) released a detailed assessment report on Qatar's

anti-money laundering / counterterrorist finance (AML/CTF) regime. The report was adopted by both MENA-FATF and the FATF.

Compared against FATF's 40 recommendations on money laundering the report found Qatar compliant on two, largely compliant on eight, partially compliant on twenty, and noncompliant on ten. For the nine special recommendations on terrorist finance, the IMF team judged Qatar as partially compliant with two, largely compliant with one, and noncompliant on six.

The Government of Qatar (GOQ) welcomed the IMF assessment and stated that it is "acutely aware of the risks attendant on a rapidly growing financial sector." The government also signaled its intention to continue developing an AML/CTF framework that is in high-level compliance with the FATF 40 plus 9 recommendations. Qatari authorities are currently drafting a new AML/CTF law and regulatory measures, implementing further supervisory measures, and creating a central committee on training to implement a comprehensive training program for all financial institutions and authorities with AML/CTF responsibilities.

The Qatar Central Bank (QCB) exercises primary regulatory authority over the financial sector. There are 18 licensed banks, including three Islamic banks and a specialized bank—the Qatar Industrial Development Bank. Qatar has 20 exchange houses, three investment companies and two commercial finance companies. Unlike most business sectors in Qatar, the Qatar Financial Center (QFC) allows major international financial institutions and corporations to set up offices with 100 percent foreign ownership. There are currently 96 firms authorized to operate in the QFC, representing a spectrum of banks, investment companies, insurance houses, and related professional services. QFC firms are limited to providing services to wholesale clients, except for insurance companies that can provide services to both wholesale and retail clients. The QFC has a separate, independent regulatory authority, the QFC Regulatory Authority. The QFC regulatory regime uses international standards. There are plans underway to create a unified regulatory authority for the country, though it remains unclear when the necessary legislation and oversight board will be in place, and also how Gulf Cooperation Council plans for a unified currency and central banking system by 2010 will affect Qatar's regulatory plans.

Qatar's anti-money laundering and counterterrorist financing (AML/CTF) legal framework is based on Law (28) of 2002 which criminalized money laundering as amended by Decree Law (21) 2003 and Law (3) of 2004 on Combating Terrorism which criminalizes terrorist financing in a limited way. The laws' effectiveness has yet to be tested, as there have been no prosecutions for money laundering or terrorist financing crimes since enactment. Authorities have investigated terrorist activity in Qatar but no measures were taken to investigate their funding. Khalifa Muhammad Turki al-Subaiy, a Qatar-based terrorist financier and facilitator, was convicted in January 2008 in absentia by the Bahraini High Criminal Court for financing terrorism and other related charges. He was subsequently arrested in Qatar where he served his six-month prison sentence from March-September 2008. On October 10, 2008, al-Subaiy was added to the UN 1267 Committee list of individuals subject to targeted sanctions.

According to Article 28 of the Anti-Money Laundering Law, money laundering offenses involve the acquisition, holding, disposing of, managing, keeping, exchanging, depositing, investing, transferring, or converting of funds from illegal proceeds. The AML law imposes fines and penalties of imprisonment of five to seven years. The AML law expands the powers of confiscation to include the identification and freezing of assets as well as the ultimate confiscation of the illegal proceeds upon conviction of the defendant for money laundering. Article two includes any activities related to terrorist financing. Article 12 authorizes the Central Bank Governor to freeze suspicious accounts for up to ten days and to inform the Public Prosecutor within three days of any action taken. The Public Prosecutor may renew or nullify the freeze order for a period of up to three months. The AML law explicitly provides for both personal and corporate liability for money laundering. The AML law requires all financial institutions to report suspicious transactions to the Financial Information Unit

and retain records for up to 15 years. The law also gives the QCB greater powers to inspect suspicious bank accounts and grants the authorities the right to confiscate money in illegal transactions. Article 17 permits the GOQ to extradite convicted criminals in accordance with international or bilateral treaties.

According to the IMF evaluation, Qatar's AML law is only partially compliant with the FATF 40 plus 9 recommendations as the effectiveness is not evidenced, it does not cover acts conducted with a view to conceal the true nature, location, disposition, movement or ownership or rights with respect to proceeds, it does not cover required predicate offenses, and it does not give authorities jurisdiction over predicate offenses that were entirely committed in another country, even if there is dual criminality.

The QFC law provides that Qatari criminal laws apply in the QFC, including those Qatari laws criminalizing money laundering and the financing of terrorism. In addition, the QFC has implemented its own anti-money laundering regulations and corresponding rules. The QFC Regulatory Authority is responsible for supervising QFC firms' compliance with QFC AML requirements. In April 2008 it issued modifications to its AML rulebook to strengthen some measures, including requiring firms to consider making a suspicious activity report if a customer fails to undergo due diligence. The revised rules also required intensified monitoring of QFC subsidiaries or branches that may be operating in other jurisdictions.

The Anti-Money Laundering Law established an interagency committee to oversee and coordinate money laundering combating efforts. The National Anti-Money Laundering and Terrorism Financing Committee is chaired by the Deputy Governor of the QCB and includes members from the Qatar Central Bank, financial intelligence unit (FIU), Ministries of Interior, Labor and Social Affairs, Business and Trade, Finance, Justice, Customs and Ports Authority and the State Security Bureau.

In February 2004, the GOQ passed the Combating Terrorism Law. According to Article Four of the law, any individual or entity that provides financial or logistical support, or raises money for activities considered terrorist crimes, is subject to punishment. The punishments are listed in Article Two of the law, which include the death penalty, life imprisonment, and 10 or 15 year jail sentences depending on the crime.

Qatar has a National Counterterrorism Committee to review the consolidated UN 1267 terrorist designation lists and to recommend any necessary actions against individuals or entities found in Qatar. The committee is chaired by the Minister of State for Interior Affairs and includes the FIU and various law enforcement representatives. The committee and the Central Bank circulate to financial institutions the individuals and entities included on the UN 1267 Sanctions Committee's consolidated list, but have thus far not identified or frozen any related assets. The IMF assessment found that overall the dissemination process is too limited and infrequent to be fully effective.

In October 2004, the GOQ established a financial intelligence unit known as the Qatar Financial Information Unit (QFIU). The FIU is responsible for receiving and reviewing all suspicious and financial transaction reports, identifying transactions and financial activities of concern, ensuring that all government ministries and agencies have procedures and standards to ensure proper oversight of financial transactions, and recommending actions to be taken if suspicious transactions or financial activities of concern are identified. The FIU also obtains additional information from the banks and other government ministries. Suspicious transaction reports (STRs) are now sent to the FIU by hardcopy or electronically, but the FIU is developing an all-electronic system with bank compliance offices that should speed the reporting process.

The QCB, Public Prosecutor and the Criminal Investigation Division (CID) of the Ministry of the Interior work together with the FIU to investigate and prosecute money laundering and terrorism finance cases. The FIU also coordinates closely with the Doha Securities Market (DSM) to establish

procedures and standards to monitor all financial activities that occur in Qatar's stock market. The FIU coordinates with the different regulatory agencies in Qatar. For example, the FIU works closely with the QFC Regulatory Authority to ensure that QFC firms, and specifically their Money Laundering Reporting Officers, understand and implement appropriate AML and counterterrorist finance policies and procedures.

The Qatari FIU became a member of the Egmont Group in 2005. The IMF assessment found the QFIU "largely compliant" but found problems with the legal basis for establishing the FIU, poor quality of STR analysis, insufficient staff, no guidance on filing STRs issued by the FIU, inadequate protection of information and facility, and no periodic review of the AML-CTF system's effectiveness. Additionally, there is no obligation in legislation for suspicious transactions related to terrorist financing to be reported.

In December 2004, the QCB installed a central reporting system. The FIU uses this system to monitor suspicious transactions reports and analyze trends. All accounts must be opened in person. Banks are required to know their customers; the banking system is considered open in that in addition to Qatari citizens and legal foreign residents, nonresidents can open an account based on a reliable recommendation from his or her primary bank. The IMF found that preventive measures for financial institutions in the domestic sector fall short of addressing a vast majority of international customer due diligence standards. For example, the current obligations do not prohibit the opening of anonymous accounts or accounts in fictitious names. Hawala transactions are prohibited by law in Qatar, though informal remittance systems do exist and the largely undocumented nature of these networks makes it difficult to judge prospective money laundering activity.

Qatar's domestic supervisory authorities, with the exception of the insurance supervisor, were judged by the IMF to possess adequate authority and powers to supervise financial institutions and ensure compliance with AML/CTF laws and regulations. The team found, however, that in practice AML/CTF inspections were inadequate, and none of the authorities had ever imposed sanctions on the institutions they supervise for noncompliance. In mid-2008, the Central Bank created an AML/CTF unit to oversee the local banking sector and liaise with compliance officers to ensure regulations were being implemented. The IMF reported that the QFC legal and regulatory framework for AML/CTF appears to be in line with the FATF standard, though the center's recent establishment and limited number of firms made it difficult for assessors to evaluate the effectiveness of the framework.

Regarding Iran-related terrorism and proliferation transactions, the Central Bank ordered financial institutions to freeze any assets of entities listed in UNSCRs 1737, 1747, and 1803, and prohibits them from carrying out any transactions with listed entities. However, Iran's Bank Saderat—an entity of concern in UNSCR 1803—was allowed to open a second branch in Doha in June 2008.

Law No. 13 from 2004 established The Qatar Authority for Charitable Activities (QACA), which monitors all charitable activity in and outside of Qatar. Only officially registered organizations can collect and disperse money for charitable purposes. There are five officially registered charities in Qatar: Qatar Charity, the Sheikh Eid Bin Mohammad Al Thani Charitable Association, the Qatari Red Crescent, the Jassim Bin Jaber Bin Mohammad Al Thani Charitable Association, and Reach Out to Asia (ROTA). Two additional charities are in the process of being registered. The Secretary General of the Authority approves all international fund transfers by the charities. The Authority reports to the cabinet via the Ministry of Labor and Social Affairs and has primary responsibility for monitoring overseas charitable, development, and humanitarian projects that were previously under the oversight of several government agencies. The IMF assessment found that domestic measures to prevent abuse of nonprofits go beyond FATF recommendations, and the QACA appears to ensure effective implementation of the requirements in place.

Overseas charitable activities must be undertaken in collaboration with a nongovernmental organization (NGO) that is legally registered in the receiving country. The Authority has a seven-

member team that travels to project sites to evaluate projects and audit their finances. The Authority prepares an annual report on the status of all projects and submits the report to relevant ministries. The Authority also regulates domestic charity collection. Article 18 of the law provides penalties of up to a year in prison, a fine of 50,000 Qatari riyals (approximately $13,750), and confiscation of the money involved for "anyone who collects donations, or transfers money outside the country, bestows or accepts loans or grants or donations or bequests or endowments" outside of the Authority's purview. The Ministry of Islamic Endowments (Awqaf) collects Islamic charitable contributions (zakat) through official collection points and administers disbursement of funds to the needy.

Qatar separates the authorities in charge of investigations and the legal authorities in charge of the judgment of criminal offenses. Qatar has designated a number of competent authorities to investigate and prosecute money laundering and terrorist financing offenses. The authorities in charge of AML/CTF investigations operate independently. Investigations are mainly the responsibility of four separate authorities: 1) the Economic Crimes Prevention Division (ECPD) within the Ministry of Interior (MOI); 2) the Public Prosecutor's Office (PPO); 3) the State Security Bureau (SSB); and 4) the Customs. The competent authorities are able to obtain documents and information for use in investigations, prosecutions, and related actions. However, the various agencies do not appear to be sufficiently structured, funded, and resourced to effectively carry out their functions. There is a lack of AML/CTF investigations, prosecutions, and convictions.

Qatar does not have mandatory cross-border currency reporting requirements. In suspicious cases, Customs officials are given authority to require travelers to fill out forms declaring cash currency or other negotiable financial instruments in their possession. Officials then forward the traveler's information to the FIU for evaluation. The IMF judged that the current system is neither implemented nor effective.

The GOQ is a party to the 1988 UN Drug Convention. The Cabinet has approved Qatar's accession to the UN Convention for the Suppression of the Financing of Terrorism and the government is finalizing necessary documentation to formally accede to the convention. Qatar is not a party to the UN Convention against Corruption. The Amir approved Qatar's accession to the UN Convention against Transnational Organized Crime and Qatar's permanent delegation to the United Nations will submit the approval document to the UN Secretary General.

The Government of Qatar should continue to implement AML/CTF policies and procedures that adhere to world standards, particularly the recommendations of the IMF review of Qatar. Per FATF Special Recommendation nine, Qatar should initiate and enforce in-bound and out-bound cross-border currency reporting requirements. The GOQ should enhance training for law enforcement, prosecutors, and customs authorities so that they can improve their capabilities in recognizing and pursuing various forms of terrorist financing, money laundering and other financial crimes. Qatar should become a party to the UN Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime.

Romania

Romania's geographical location makes it a natural transit country for trafficking in narcotics, arms, stolen vehicles, and persons by transnational organized criminal elements. As such, the nation is vulnerable to financial activities associated with such crimes, including money laundering. Trans-border smuggling of counterfeit goods, tax fraud, and fraudulent claims in relation to consumer lending are additional types of financial crimes prevalent in Romania. Romania also has one of the highest rates of cybercrime and online credit card fraud in the world. Recent studies have found Romanian servers to be the second largest source (13 percent) of cybercrime transactions worldwide. Although a majority of their victims reside in the United States, Romanian cyber-criminals are increasingly targeting victims elsewhere in Europe as well as in Romania itself.

Laundered money comes primarily from international crime syndicates who conduct their criminal activity in Romania and subsequently launder their illicit proceeds through illegitimate front companies. Another source of laundered money is the proceeds of illegally smuggled goods such as cigarettes, alcohol, gasoline, and other dutiable commodities. Corruption in Romania's customs and border control authorities coupled with corruption in several neighboring Eastern European countries also facilitates money laundering.

Romania's Law No. 21/99, On the Prevention and Punishment of Money Laundering, criminalizes money laundering and requires customer identification, record keeping, suspicious transaction reporting, and currency transaction reporting for transactions (including wire transfers) over 10,000 euros (approximately $13,500). In 2008, this threshold is increased to 15,000 euros (approximately $20,250) by Government of Romania (GOR) Emergency Ordinance 53/2008. The list of entities covered by Law No. 21/99 includes banks, nonbank financial institutions, attorneys, accountants, and notaries. The Law on the Prevention and Sanctioning of Money Laundering (Law 656/2002) expands the list of predicate offenses to include all crimes and expands the number and types of entities subject to anti-money laundering (AML) regulations. The additional entities include art dealers, travel agents, privatization agents, postal officials, money service businesses, and real estate agents. Although nonbank financial institutions are covered under Romania's AML laws, regulatory supervision of this sector is weak and not as rigorous as that imposed on banks. Romania also has criminalized tipping off. Romanian law permits the disclosure of client and ownership information to bank supervisors and law enforcement authorities. Safe harbor provisions protect banking officials when they cooperate with law enforcement. In 2003, Romania instituted an anticorruption plan and passed a law criminalizing organized crime.

In keeping with international standards, Romania has taken steps to strengthen its know your customer (KYC) identification requirements. The National Bank of Romania's (BNR) 2003 Norm No. 3, "Know Your Customer," strengthens information disclosure requirements for incoming and outgoing wire transfers by requiring banks to include information about the originator's name, address, and account. It also strengthens correspondent banking practices by requiring banks to undertake proper due diligence measures before entering into international correspondent relations, and prohibiting them from opening correspondent accounts with shell banks. In 2006, the BNR widened the scope of its KYC norms by extending their application to all other nonbanking financial institutions falling under its supervision. The Insurance Supervision Commission has instituted similar regulations for the insurance industry. Despite these enhancements to existing regulations, Romania is still deficient in implementing customer due diligence (CDD) requirements, as noted during the 2007 mutual evaluation by the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), a Financial Action Task Force (FATF)-style regional body. Romanian law still has no explicit definition of beneficial ownership. In addition, the requirement to take reasonable measures to verify the identity of the beneficial owner, as required by international standards, has not yet been adequately implemented.

In 2005, Romania modified its money laundering legislation with Law 230/2005. This law provides a uniform approach to combating and preventing money laundering and terrorist financing. The modified law establishes a suspicious transaction reporting (STR) requirement for transactions linked to terrorist financing. The reporting requirement, however, is incomplete in its current form, and needs to be further developed in order to fully comply with FATF standards.

In 2006, Romania made further changes to its laws. These changes increase fines to match the inflation rate, allow the use of undercover investigators, and permit the submission of reports from the financial intelligence unit (FIU) to the General Prosecutor's Office (GPO) in an unclassified manner. The changes also provide for confiscation of goods used in or resulting from money laundering activities, and increase the length of time that bank accounts may be frozen from ten days to one month.

The GOR passed two new laws in 2008. The new legislation amends Law 656/2002 to provide stricter definitions for "real end-user," "transactions that seem to be inter-connected," "fictitious bank," and the "external transfer" concept. The laws also clarify the process whereby the FIU issues feedback to reporting entities, includes simplified and supplementary KYC measures, and contains prohibitions on operating anonymous accounts or conducting business relations with a fictitious bank. Finally, the new legislation clarifies that the BNR is the competent supervisory authority for all credit/lending institutions in terms of reporting, while the FIU has this authority for any other entity carrying out money transfers. The law also establishes new requirements for monthly reporting by the National Customs Authority to the FIU of all available data regarding cross-border cash declarations. The FIU's Governing Board has issued regulations implementing KYC standards for nonfinancial reporting entities (casinos, notaries, real estate brokers). These norms bring previously unsupervised entities under supervision for compliance with AML regulations. In addition to the FIU, Romanian state institutions, including the BNR and the National Securities Commission have been quick to apply these new laws by issuing implementing regulations.

Romania's FIU, the National Office for the Prevention and Control of Money Laundering, was established in 1999. All obliged entities must submit their currency transaction reports (CTRs) and STRs to the FIU. The FIU oversees the implementation of AML guidelines for the financial sector and works to ensure that all domestic financial institutions covered by the law receive adequate training. The FIU also is authorized to participate in inspections and controls in conjunction with supervisory authorities. In the first ten months of 2007, the FIU carried out 189 on-site inspections in cooperation with the Financial Guard or other supervisory authorities, an increase from the 109 inspections for the same period in 2006.

To further its attempt to enhance supervision of entities that are not formally supervised for AML compliance by another agency, the FIU's Governing Board issued a decision in January 2008, outlining procedures for carrying out its supervisory authorities over nonfinancial reporting entities such as casinos, real estate brokers, and nongovernmental organizations (NGOs). Using these new procedures, the FIU, in the first nine months of 2008, conducted off-site supervision inspections of 1,329 firms in the gaming industry, 990 real estate brokers, and 3,282 NGOs. During this same time period, the FIU conducted on-site inspections of 167 other reporting entities, of which 112 were penalized with fines totaling RON 235,000 (approximately $81,000). An additional 128 warnings were issued. Out of the 167 on-site inspections, 127 were carried out solely by the FIU, three jointly with the BNR, and 37 jointly with the Financial Guard.

During the first nine months of 2008, the FIU received 61,372 CTRs, a substantial increase from the 10,747 CTRs received in the first ten months of 2007. During the same period in 2008, the FIU received 1,452 STRs, down from 1,542 reports during the same period in 2007, and 2,218 STRs in 2006. The FIU received 6,402 reports of cross-border transfers during the first nine months of 2008, compared with 6,511 reports during the same period in 2007. The majority of these reports were submitted by credit institutions, casinos, public notaries, and money transfer agencies. Financial investment institutions, nonbanking financial institutions, fiscal consultants, insurance and re-insurance companies, real estate brokerage firms, individual and corporate retailers, NGOs, and lawyers were among other entities also submitting reports. Also during the first nine months of 2008, the FIU received 352 notifications concerning suspicions of money laundering and terrorist financing from agencies as varied as the BNR, the Insurance Supervision Commission, the Ministry of Economy and Finance, and the Financial Guard.

After reviewing and analyzing the submitted reports, the FIU forwards its findings to the appropriate government agency for follow-up investigation. During the first nine months of 2008, the FIU completed 965 cases: 496 (489 money laundering/seven terrorist financing) of those cases were forwarded.

Since its establishment, the FIU has faced numerous political and operational challenges, including low staffing levels as well as criminal charges of corruption against a former FIU official. The FIU also has been criticized by the GPO for forwarding poor quality reports to prosecutors. Consequently, coordination between the FIU and law enforcement has often suffered. In its 2007 evaluation of Romania, MONEYVAL cites the existence of a backlog of STRs still needing analysis. Despite these setbacks, the FIU is working to improve its operations and is currently seeking to place an emphasis on quality rather than quantity when analyzing suspicious transactions. The FIU believes the number of indictments and eventual convictions will increase over time as a greater emphasis is placed on the quality of reports produced as opposed to the quantity of reports forwarded to the GPO. The FIU has improved the timeliness and quality of its analysis and case reporting. However, investigations have resulted in only a handful of successful prosecutions to date.

Throughout 2008, the FIU has sought to bolster cooperation with the GPO, as well as the BNR, National Anti-Drug Agency, Ministry of Interior, National Magistracy Institute, and Ministry of Foreign Affairs. In July 2008, the FIU organized a national conference to highlight Romania's full harmonization with European Union (EU) legislation. In addition, the FIU is partnering with the EU through a PHARE (Poland-Hungary Assistance for Reconstruction of the Economy) project. This project has several components: development of a secured IT data transfer system; establishment of a case management system; purchase of accredited hardware and software; and creation of a system for data recovery in case of disasters. The FIU is also working on another AML development program with Poland through an EU Twinning project.

Efforts to prosecute cases have been hampered by the lack of specialization and technical knowledge of financial crimes within the judiciary. Despite a low number of convictions, coordination between law enforcement and the justice system continues to improve. In the first nine months of 2008, the Directorate for the Investigation of Organized Crime and Terrorism Offenses (DIICOT), a division of the GPO, indicted 41 defendants in five cases involving money laundering. Funds and goods totaling 50 million Euros (approximately $65,500,000) have been seized or frozen. Of the 41 indicted, eight defendants have been placed under preventive arrest. During the first nine months of 2008, DIICOT opened criminal investigations on 112 files involving suspicion of money laundering.

In response to the events of September 11, 2001, Romania passed a number of legislative measures designed to criminalize acts contributing to terrorism. Emergency Ordinance 141, passed in October 2001, provides that the production or acquisition of means or instruments, with intent to commit terrorist acts, are offenses of exactly the same level as terrorist acts themselves. These offenses are punishable with imprisonment ranging from five to 20 years. The Supreme Defense Council of the Country has adopted a National Security Strategy, which includes the General Protocol on the Organization and Functioning of the National System on Preventing and Combating of Terrorist Acts. This system, effective July 2002, and coordinated through the Intelligence Service, brings together and coordinates a multitude of agencies, including 14 ministries, the GPO, the BNR, and the FIU. The GOR also has set up an inter-ministerial committee to investigate the potential use of the Romanian financial system by terrorist organizations. A revised Criminal Procedure Code entered into force in July 2003, containing provisions for authorizing wiretaps, and intercepting and recording telephone calls in money laundering and terrorist financing cases.

Romanian law has some limited provisions for asset forfeiture in the Law on Combating Corruption, No. 78/2000, and the Law on Prevention and Combat of Tax Evasion, No. 241, introduced in July 2005. The GOR, and particularly the BNR, has been cooperative in seeking to identify and freeze terrorist assets. Emergency Ordinance 159, passed in late 2001, includes provisions for preventing the use of the financial and banking system to finance terrorist attacks and sets forth the parameters for the government to combat such use. The GOR Emergency Ordinance 153 strengthens the government's ability to carry out its obligations under UNSCR 1373, including the identification, freezing, and seizure of terrorist funds or assets. Legislative changes in 2005 extend the length of time a suspect

account may be frozen. The FIU is now authorized to suspend accounts suspected of money laundering activity for three working days, as opposed to the previous two-day limit. In addition, once the case is sent to the GPO, it may further extend the period by four working days instead of the previously allowed three working days.

Law 535/2004 on preventing and combating terrorism abrogates some of the previous government ordinances and incorporates many of their provisions. The law includes a chapter on combating the financing of terrorism by prohibiting financial and banking transactions with persons included on international terrorist lists, and requiring authorization for transactions conducted with entities suspected of terrorist activities in Romania.

The BNR receives lists of individuals and terrorist organizations provided by the United States, the UNSCR 1267 Sanctions Committee, and the EU, and it circulates these to banks and financial institutions. The law on terrorism provides for the forfeiture of assets used by or provided to terrorist entities, together with finances resulting from terrorist activity. To date, no terrorist financing arrests, seizures, or prosecutions have been reported.

The FIU is aware of the potential misuse of charitable or nonprofit entities as conduits for terrorist financing. In 2007, the FIU conducted two training events with charitable foundations and associations on preventing and combating money laundering and terrorist financing. The FIU has drafted guidelines concerning reporting entities' obligations in this respect and has published them on its website.

The GOR recognizes the link between organized crime and terrorism. Romania is a member of and host country for the headquarters of the Southeast European Cooperative Initiative's (SECI) Center for Combating Trans-border Crime, a regional center that focuses on intelligence sharing related to criminal activities, including terrorism. Romania also participates in a number of regional initiatives to combat terrorism. Romania has worked within the South East Europe Security Cooperation Steering Group (SEEGROUP), a working body of the NATO initiative for Southeast Europe to coordinate counterterrorist measures undertaken by the states of southeastern Europe. The Romanian and Bulgarian Interior Ministers have signed an inter-governmental agreement to cooperate in the fight against organized crime, drug smuggling, and terrorism.

The FIU is a member of the Egmont Group, and the GOR is a member of MONEYVAL. The most recent MONEYVAL mutual evaluation of Romania, conducted in May 2007, was adopted at the group's plenary in July 2008. Its final report, published in October 2008, concludes that Romania made significant progress since its previous evaluation in 2003. Taking into account the report recommendations, Romanian institutions with specific duties will carry out an action plan to implement the recommendations, with results to be discussed by MONEYVAL in 2009.

A Mutual Legal Assistance Treaty between the United States and Romania entered into force in October 2001. The GOR has demonstrated its commitment to international anti-crime initiatives by participating in regional and global anti-crime efforts. Romania is a party to the 1988 UN Drug Convention, the UN Convention against Corruption, the UN Convention against Transnational Organized Crime and the UN Convention for the Suppression of the Financing of Terrorism. The FIU has signed 42 bilateral memoranda of understanding with Egmont Group member FIUs. Romania's FIU shares information internationally and is a member of the FIU.Net network. In the first nine months of 2008, Romania's FIU sent 328 data requests to FIUs abroad and received 83 similar requests from external FIU partners. Romania's FIU received 15 data requests from abroad regarding suspicions of terrorist financing. However, no actual operations suspected of terrorist financing have been identified.

While Romania's AML legislation and regulations will soon be compliant with many FATF Recommendations, implementation has moved at a slower pace. With the conclusion of the Romanian

capital account liberalization in 2006, the risk of money laundering through nonbank entities has been on the rise. The Government of Romania should continue its efforts to ensure that nonbank financial institutions are adequately supervised. Additionally, the knowledge level of the sector should be increased regarding its reporting and record keeping responsibilities and the identification of suspicious transactions. The GOR should continue to improve communication between reporting and monitoring entities, as well as between prosecutors and the FIU. The GPO should continue to place a high priority on money laundering cases. Romania should improve implementation of existing procedures for the timely freezing, seizure, and forfeiture of criminal or terrorist-related assets. Romania should continue to make progress in combating corruption in commerce and government. The GOR should enact and implement legislation to subject NGOs and charitable organizations to reporting requirements.

Russia

As the world's geographically largest country, Russia has worked towards creating a liberal market economy. Although it is a regional financial center, its financial system does not attract a significant number of depositors. However, due to rapid economic growth in various sectors, the number of depositors has been increasing steadily. Experts believe that most of the illicit funds flowing through Russia derive from domestic criminal activity, including evasion of tax and customs duties, fraud, public corruption, and smuggling. Russian authorities recently described more than 120 money laundering typologies used in Russia, including account fraud, front companies and identity fraud, multiple transactions through a network of off-shore firms, back-to-back loans, and disguising illegal proceeds as gains of gambling activities. Criminals invest and launder their proceeds in real estate and security instruments, or use them to buy luxury consumer goods. Criminal elements from Russia and neighboring countries continue to use Russia's financial system to launder money because of their familiarity with the language, culture, and economic system. Despite making progress in combating financial crimes, Russia remains vulnerable to such activities because of its vast natural resource wealth and associated large-scale financial transactions, the pervasiveness of organized crime, the heavy direct and indirect role of the state in the economy, and an admitted high level of corruption. Other vulnerabilities include porous borders, Russia's role as a geographic gateway to Europe and Asia, a weak banking system that attracts little public confidence, and under-funding of regulatory and law enforcement agencies, which contributes to both corruption and lack of regulatory and law enforcement capacity. Russia's financial intelligence unit (FIU) estimates that Russian citizens may have laundered as much as U.S. $370 billion in 2008.

The Russian Federation has a legislative and regulatory framework in place to pursue and prosecute financial crimes, including money laundering and terrorist financing. Russia's anti-money laundering and counterterrorist financing (AML/CTF) regime underwent a joint evaluation by the Financial Action Task Force (FATF) and two of the FATF-style regional bodies, the Eurasian Group on Combating Money Laundering and the Financing of Terrorism (EAG) and the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) in the fourth quarter of 2007. The three plenary bodies adopted the mutual evaluation report (MER) in June and July 2008.

Russia takes an "all crimes" approach to money laundering predicate offenses, and criminalizes money laundering by articles 174 of the Criminal Code (CC) (money laundering), 174.1 CC (self-laundering) and 175 CC (acquisition of property obtained by crime). The elements in these provisions are consistent with the requirements of the Vienna and Palermo Conventions. According to the 2008 MER, Russia is largely compliant with the FATF recommendations on criminalization of money laundering and has progressively improved implementation of its AML regime. Russia has criminalized self- laundering and the acquisition of property obtained by crime. The maximum

criminal penalty for natural persons convicted of money laundering or financing terrorism is 10 years in prison in addition to applicable fines

Although legal persons are not subject to criminal liability, Russian law provides for corporate and administrative liability for legal persons.

Various regulatory bodies ensure compliance with Russia's AML/CTF laws. The Central Bank of Russia (CBR) supervises credit institutions; the Federal Insurance Supervision Service (FISS) oversees the insurance sector and the Federal Service for Financial Markets (FSFM) regulates entities managing nongovernmental pension and investment funds, as well as professional participants in the securities sector. The Assay Chamber (under the Ministry of Finance) supervises entities engaged in trade in precious metals and stones. The Federal Financial Monitoring Service (FFMS, also known as Rosfinmonitoring) regulates real estate and leasing companies, pawnshops, payment acceptance and money transfer services, and participants in the gaming industry. The Federal Service of Supervision in the sphere of Mass Communications, Communications and Protections of Cultural Heritage, also known as Roscommunication or ROSCOM, is the supervisory body for Russia Post, including the Russia Post's compliance with the AML/CTF Law. The Federal Registration Service (ROSREG) is responsible for registration of real estate ownership (land registry), political parties and public associations (and other related state registers) and other legal entities, except for commercial entities that register with the Federal Tax Service (FTS). The FTS exercises supervision over currency operations and lotteries under the authority of the Ministry of Finance (MoF). While the supervision carried out by the Bank of Russia is thorough and effective, the MER indicated that the authorities do not adequately inspect the securities and insurance sectors, nor do supervisors have adequate sanctions powers to correct compliance shortcomings.

The legal framework for customer due diligence is set out in a variety of legal documents. The AML Law (Law 115-FZ), introduced in 2001, obliges banking and nonbanking financial institutions to monitor and report certain types of transactions, maintain records, and identify their beneficiary customers. According to RF 115-FZ, institutions legally required to report include banks, credit organizations, securities market professionals, insurance and leasing companies, the federal postal service, jewelry and precious metals merchants, betting shops, and companies managing investment and nongovernmental pension funds. Other obliged entities include real estate agents, lawyers and notaries, and persons rendering legal or accounting services that involve certain transactions. The law also requires banks to identify customers before providing natural or legal persons with financial services. However, while banks are explicitly prohibited from opening anonymous accounts, there is no specific provision that prohibits them from maintaining existing accounts under fictitious names. The CBR has issued guidelines regarding AML practices within credit institutions, including "know your customer" (KYC) and bank due diligence programs. Banks must obtain information regarding individuals, legal entities and the beneficial owners of corporate entities and retain it for a minimum of five years from the date of the termination of the business relationship. Banks must also adopt internal compliance rules and procedures and appoint compliance officers. According to the MER, record keeping requirements are generally comprehensive and are largely compliant with FATF recommendations. Particular areas of concern involve the uneven approach among financial institutions to identification of the beneficial owner and inconsistent requirements in performing ongoing due diligence.

Except for attempted transactions by occasional customers, financial institutions must report all suspicious transactions relating to money laundering. Financial institutions are also required to file a Suspicious Transaction Report (STR) if there is a suspicion of financing of terrorism. In addition, financial institutions are required to report certain large value transactions (equal to or exceeding RUB 600,000) to the FIU. Financial institutions that fail to meet large value or suspicious transaction reporting requirements face possible license revocation or liquidation through civil proceedings. The maximum criminal penalty for natural persons convicted of money laundering or financing terrorism

is 10 years in prison, in addition to applicable fines.

All obligated financial institutions must monitor and report to the government any transaction that equals or exceeds 600,000 rubles (approximately $22,700) and involves or relates to cash payments, remittances, bank deposits, gaming, pawn shop operations, precious stones and metals transactions, payments under life insurance policies, or persons domiciled in countries determined by the Russian Government to be deficient in AML/CTF. Obligated institutions must also report real estate transactions valued at 3,000,000 rubles (approximately $115,400) or more. Financial institutions must develop criteria for determining suspicious transactions and report such transactions to the FIU in a timely fashion. All transactions involving an entity or person included on the Russian government's list of those involved in extremist activities or terrorism must be reported to the FIU annually.

Under Order 1317-U, Russian financial institutions must inform the CBR when it establishes correspondent relationships with nonresident banks operating in offshore zones (as defined by the Russian Federation in Annex 1 of this Order). The CBR recommends that financial institutions apply enhanced due diligence to transactions with nonresident institutions. Foreign banks may only open subsidiary operations on the territory of Russia and may not open branches. The CBR must authorize the establishment of a subsidiary operation, and these subsidiaries must be subject to domestic Russian supervisory authorities. Russian banks must obtain CBR approval to open operations abroad.

According to the Law No. 395-I "On Banks and Banking Activities," credit institutions must identify and inform the CBR of all appointments of individuals to senior management positions and to the managing and supervisory boards. Russian law prohibits the appointment of anonymous parties or proxy individuals to a credit institution's managing or supervisory board. The CBR has the authority to deny the appointment of a senior official if the official does not meet "fit and proper" requirements established by the CBR, but Russia has not taken legal steps to provide supervisors the power to prevent criminals from controlling financial institutions.

Article 8 of Law 115-FZ provided for the 2001 establishment of Rosfinmonitoring. As the FIU, it is the cornerstone of the country's AML/CTF regime. It is the central policy coordinating body for AML/CTF issues, as well as the designated authority for collecting, processing, analyzing and disseminating STRs and other AML/CTF-related reports. Established as an independent government authority in 2001, Rosfinmonitoring moved directly under the Office of the Prime Minister in September 2007. It enjoys full operational autonomy.

Rosfinmonitoring has the authority to gather information regarding the activities of reporting entities. Nearly all financial institutions submit reports to the FIU via encrypted software provided by Rosfinmonitoring. The FIU maintains the national AML/CTF database that contains more than 14 million reports. Rosfinmonitoring receives approximately 30,000 transaction reports daily. It provides information and analysis to the appropriate law enforcement authorities for further investigation, including the Economic Crimes Unit of the Ministry of Interior (MVD) for criminal matters, the Federal Drug Control Service (FSKN) for narcotics-related activity, or the Federal Security Service (FSB) for terrorism-related cases. As an administrative unit, it has no law enforcement or investigative powers.

The head of Rosfinmonitoring chairs an Interagency Commission on Money Laundering, which is responsible for monitoring and coordinating the government's activity on money laundering and terrorist financing. Twelve ministries and government departments sit on the Commission.

Rosfinmonitoring has regional offices in all federal districts, with headquarters located in Moscow. Its headquarters has established a sophisticated information technology infrastructure that enables the regional offices to analyze STRs, use the national AML database and submit cases for dissemination to headquarters. The FIU demands high professional standards of its employees, and uses internal

control systems to protect information from unauthorized access by the staff. The only shortcoming detected by the FATF evaluation team was a high number of staff vacancies, especially in the analytical and supervisory departments. The regional offices also coordinate the efforts of the CBR and other supervisory agencies to implement AML/CTF regulations.

Between January 1 and the end of October 2008, the Interior Ministry registered 7,816 crimes involving money laundering. Interior Ministry official reports show that 5,802 of the cases went to trial. Both Rosfinmonitoring and MVD report that the number of STRs for the year roughly equaled those of 2007 and credit increased cooperation among law enforcement agencies for the number of cases brought to trial.

With its legislative and enforcement mechanisms in place, Russia has begun to prosecute high-level money laundering cases. As of December 1, 2008, the CBR revoked the licenses of 25 banks for failing to observe banking regulations. Of these, 20 banks lost their licenses for violating Russia's AML laws. The CBR's initiative to prohibit individuals convicted of money laundering from serving in leadership positions in the banking community—a cause championed by Andrey Kozlov, the First Deputy Chairman of the CBR who was assassinated in 2006—remains pending.

Russian legislation provides for the tracking, seizure and forfeiture of all criminal proceeds, not just those linked to narcotics-trafficking. Russian law also provides law enforcement bodies the authority to use investigative techniques such as search, seizure, and the identification, freezing, seizing, and confiscation of funds or other assets. Authorities can compel individuals to produce documents related to criminal activity, including money laundering. Investigators and prosecutors can apply to the court to freeze or seize property obtained as the result of crime, although there are some exceptions in the law restricting seizure of property identified as a primary residence. Law enforcement agencies have the power to identify and trace property that is, or may become, subject to confiscation or is suspected of being the proceeds of crime or terrorist financing. Since January 1, 2007, Russia has been using two instruments for confiscations: the Code of Criminal Procedure (CCP) Article 81, and the Criminal Code (CC) Articles 104.1 and 104.2. Both articles 81 and 104.1 provide for the confiscation of instruments, equipment or other means of committing an offense or intended to be used to commit a crime.

Russia criminalized terrorist financing in article 205.1 CC27, which targets any support or contribution to terrorist activity, including the financing of terrorism. The terrorist financing offense covers the provision and collection ("raising") of funds. Russia's treatment of the criminalization of terrorist financing comports with international law, with the exception of its failure to cover the theft of nuclear material, as required by UN Convention.

Russia has established a system for freezing terrorist assets to comply with United Nations Security Council Resolutions (UNSCRs) 1267 and 1373 and subsequent resolutions. Russia maintains both a domestic and international terrorist list. Supervisors disseminate these lists of designated terrorist entities to all reporting institutions, and authorities freeze all assets of terrorists or terrorist organizations listed in UNSCR 1267, as well as all assets belonging to persons and organizations owned or controlled by them. Assets of UN-listed (international) terrorists remain frozen until there is a de-listing by the UN. Russian authorities also identify and designate entities and individuals in accordance with AML/CTF law and regulations, and include them on the Russian domestic list. Designation on the domestic terrorist list subjects a listed entity to a temporary asset freeze. According to the AML/CTF law, financial institutions must freeze transactions suspected of involvement in terrorism finance for up to two days and report the transaction to the FIU. Rosfinmonitoring may extend the freeze by an additional five days. A court order is required to extend the freeze beyond seven days.

Rosfinmonitoring reports that it is monitoring 1,300 entities suspected of financing terrorism, including over 900 Russian citizens, 170 Russian organizations, and over 200 foreign entities. At the

request of the General Prosecutor's Office, the Russian Supreme Court has, to date, authorized an official list of 17 terrorist organizations. Russia also relies on bilateral agreements to designate entities mutually determined to be involved in extremist or terrorist activity.

In accordance with international agreements, Russia recognizes rulings of foreign courts relating to the confiscation of proceeds from crime within its territory and can transfer the confiscated proceeds of crime to the foreign state whose court issued the confiscation order.

The United States and Russia signed a Mutual Legal Assistance Treaty in 1999, which entered into force on January 31, 2002. Although Russia has assisted the U.S. in investigating cases involving terrorist financing, Russia and the U.S. continue to have differing opinions regarding the purpose of the UN 1267 Sanctions Committee's designation process. These political differences have hampered bilateral cooperation in this forum. U.S. law enforcement agencies exchange operational information with their Russian counterparts on a regular basis.

Russia is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. Russia is a member of the FATF, MONEYVAL, and EAG, which it also co-founded. The EAG Secretariat is located in Moscow. Rosfinmonitoring has established the International Training and Methodological Center of Financial Monitoring (ITMCFM) that exists to provide technical assistance, primarily in the form of staff training for FIUs and other interested ministries and agencies involved in AML/CTF efforts in the region. The ITMCFM also conducts research on AML/CTF issues and provides direct technical assistance to EAG members. As Chair of the EAG, Russia's FIU continues to play a strong leadership role in the region. Rosfinmonitoring is a member of the Egmont Group and has signed cooperation agreements with the FIUs of 24 countries, including the United States.

Through aggressive enactment and implementation of comprehensive AML/CTF legislation, the Government of Russia (GOR) has established legal and enforcement frameworks to deal with money laundering and terrorist financing. Russia has also contributed to improving the region's capacity for countering money laundering and terrorist financing. Nevertheless, serious vulnerabilities remain. Russia is home to some of the world's most sophisticated perpetrators of fraud and money laundering, who rely heavily on electronic and Internet-related means. Although Russia is increasing its money laundering prosecutions, considering the acknowledged level of organized crime and corruption in the country, Russia should continue to aggressively pursue this offense. To prevent endemic corruption and deficiencies in the business environment from undermining Russia's efforts to establish a well-functioning anti-money laundering and counterterrorism finance regime, Russia should examine and implement measures to bring down the high levels of corruption in both the public and private sectors and increase transparency in the financial sector. Russia has an incomplete legal framework with regard to politically exposed persons (PEPs), and authorities should strengthen it by addressing the shortcomings and pursuing effective implementation as soon as possible. Russia should criminalize insider trading and market manipulation. Where AML/CTF awareness is low, primarily outside the formal financial sector, authorities should issue guidance for filing STRs, in particular STRs related to terrorist financing. Russia should also improve federal oversight of shell companies and scrutinize more closely those banks that do not carry out traditional banking activities. Russia should commit adequate resources to its regulatory and law enforcement entities to enable them to fulfill their responsibilities. The GOR should also ensure that its institutions have the resources, both human and financial, to implement the law. Finally, Russia should continue to play a leadership role through sustained involvement in the regional and international bodies focusing on AML/CTF regime implementation.

Samoa

Samoa does not have major organized crime, fraud, or drug problems. The most common crimes that generate revenue within the jurisdiction are primarily the result of low-level fraud and theft. However, according to law enforcement intelligence sources, criminal organizations based in Hawaii and California are involved in the trafficking of cocaine, MDMA and crystal methamphetamine into the island nations including Samoa. Additionally, South American and Australian based organizations use the South Pacific islands as transshipment locations for cocaine being shipped from South America into Australia and New Zealand.

The domestic banking system is very small, and there is relatively little risk of significant money laundering derived from domestic sources. Samoa's offshore banking sector is relatively small. The Government of Samoa (GOS) initially enacted the Money Laundering Prevention Act in 2000 that was repealed and replaced by the new Money Laundering Prevention Act 2007. This law criminalizes money laundering associated with numerous crimes sets measures for the prevention of money laundering and requires related financial supervision. Under the Act, a conviction for a money laundering offense is punishable by a fine not to exceed Western Samoa Tala (WST) one million (approximately U.S. $354,000), a term of imprisonment not to exceed seven years, or both. This penalty is not found in the 2007 Act itself, but derives from the separate Proceeds of Crime Act of 2007, which includes specific penalties for money laundering.

The Act requires financial institutions to report transactions considered suspicious to the Samoa Financial Intelligence Unit (FIU) established by the Money Laundering Prevention Authority (MLPA) presently under the auspices of the Governor of the Central Bank. The FIU receives and analyzes disclosures from either a local financial or government institution or agency (either domestic or of a foreign state). If it establishes reasonable grounds to suspect that a transaction is suspicious, it may disclose the report to an appropriate local or foreign government or law enforcement agency. A Money Laundering Prevention Task Force (MLPTF) was established in 2007, which meets quarterly, under the new Act to advise or make recommendations to the MLPA. The task force consists of heads from the Central Bank, Attorney General, Police Force, Samoa International Finance Authority (SIFA), Ministry of the Prime Minister and FIU. More importantly, the MLPTF is tasked to ensure close liaison and cooperation and coordination between various GOS departments and corporations. In ensuring this, the task force established a Memorandum of Understanding (MOU) between the FIU and all members of the Task Force with respect to formal exchange and sharing of relevant information to counter money laundering offenses and terrorist financing activities. In 2003, the GOS established under the authority of the Ministry of the Prime Minister an independent and permanent Transnational Crime Unit (TCU). The TCU is staffed by personnel from the Samoa Police Service, Immigration Division of the Ministry of the Prime Minister and Division of Customs. The TCU is responsible for intelligence gathering and analysis and investigating transnational crimes, including money laundering, terrorist financing and the smuggling of narcotics and people.

Further, the Act requires financial institutions to establish and maintain with appropriate backup or recovery all business transactions records and correspondence records for a minimum of five years, and to identify and verify a customer's identity when establishing a business relationship; when there is a suspicion of a Money Laundering offense or terrorist financing; or when there is doubt about the veracity or adequacy of the customer identification, or verification, documentation, or information previously obtained.

Section 31 of the Act requires that all financial institutions have an obligation to appoint a compliance officer responsible for ensuring compliance with the Act, and to establish and maintain procedures and systems to implement customer identification requirements, implement record keeping, retention, and reporting requirements and to make its officers and employees aware of procedures, policies and audit systems. Each financial institution is also required to train its officers, employees and agents to

recognize suspicious transactions. A financial institution required to be audited must incorporate compliance with the MLPA 2007 as part of its audit to be confirmed by the auditor. Currency reporting at the border requires any person leaving or entering Samoa with more than $20,000 or other prescribed amount in cash or negotiable bearer instruments (in Samoan currency or equivalent foreign currency) either on their person or in their personal luggage to report this to the FIU.

The Act removes secrecy protections and prohibitions on the disclosure of relevant information. Moreover, it provides protection from both civil and criminal liability for disclosures related to potential money laundering offenses to the competent authority.

The Central Bank of Samoa, the SIFA, and the MLPA regulate the financial system. There are four locally incorporated commercial banks, supervised by the Central Bank. The SIFA has responsibility for regulation and administration of the offshore sector. There are no casinos, but two local lotteries are in operation.

Samoa is an offshore financial jurisdiction with six offshore banks licensed. For entities registered or licensed under the various Offshore Finance Centre Acts, there are no currency or exchange controls or regulations, and no foreign exchange levies payable on foreign currency transactions. No income tax or other duties, nor any other direct or indirect tax or stamp duty is payable by registered/licensed entities. In addition to the six offshore banks, Samoa currently has 27,039 international business corporations (IBCs) four international insurance companies, seven trustee companies, and 182 international trusts. Section 19 of the International Banking Act requires the directors and Chief Executive to be "fit and proper" and prohibits any person from applying to be a director, manager, or officer of an offshore bank who has been sentenced for an offense involving dishonesty. The prohibition is also reflected in the application forms and personal questionnaire that are completed by prospective applicants that detail the licensing requirements for offshore banks. The application forms list the required supporting documentation for proposed directors of a bank. These include references from a lawyer, accountant, and a bank, police clearances, curriculum vitae, certified copies of passports, and personal statements of assets and liabilities (if also a beneficial owner). The Inspector of International Banks must be satisfied with all supporting documentation that a proposed director is "fit and proper" in terms of his integrity, competence and solvency, which is defined in section 3 of the Act.

International cooperation can occur in several ways under the provisions of three pieces of legislation: the Money Laundering Prevention Act 2007, the Proceeds of Crime Act 2007, and Mutual Assistance in Criminal Matters Act 2007. All cooperation under the MLPA is through the FIU under the new Money Laundering Prevention Act 2007, which allows exchange of information not only on a national but also on an international basis between the FIU and other domestic law enforcement and regulatory agencies. Under the Proceeds of Crime Act 2007, a foreign State can request assistance to issue a restraining order in respect of a foreign serious offense. The Attorney General under the Mutual Assistance in Criminal Matters Act 2007 can authorize the giving of assistance to a foreign state. Assistance to a foreign state can be in the form of locating or identifying persons or providing evidence or producing documents or other articles in Samoa. In 2002, Samoa enacted the Prevention and Suppression of Terrorism Act. The Act defines and criminalizes terrorist offenses, including offenses dealing specifically with the financing of terrorist activities. The combined effect of the Money Laundering Prevention Act of 2007 and the Prevention and Suppression of Terrorism Act of 2002 is to make it an offense for any person to provide assistance to a criminal to obtain, conceal, retain or invest funds or to finance or facilitate the financing of terrorism.

Samoa is a member of the Asia/Pacific Group on Money Laundering and the Pacific Islands Forum. In August 2004, Samoa hosted the annual plenary of the Pacific Islands Forum. Samoa has not signed the 1988 UN Drug Convention or the UN Convention against Transnational Organized Crime. However, Samoa became a party to the UN International Convention for the Suppression of the Financing of

Terrorism in 2002. The FIU and the Ministry of Foreign Affairs and Trade do issue and provide to all financial institutions governed under the Money Laundering Prevention Act 2007, an update list concerning Al-Qaida and the Taliban, and Associated Individuals and Entities in pursuant to the United Nations Security Council Resolution 1267. Financial institutions are required to check their records of customers, names and accounts and to take immediate actions to freeze or confiscate funds and promptly advise the FIU.

The FIU within the Central Bank has continued to strengthen its anti-money laundering regime as evident in the new Money Laundering Prevention Act 2007. The new Act is explicitly mandates that all financial institutions conduct customer due diligence and prohibit any transactions where there is no satisfactory evidence of a customers identity. A financial institution is obliged to keep records of all business transaction records and related correspondence, records of a customer's identity, and of all reports made to the FIU, and any enquiries made to it by the FIU on money laundering and terrorist financing matters. Anonymous accounts are strictly prohibited, and transactions are required to be monitored by financial institutions. The scope of record keeping by financial institutions (like banks and money transmission service providers) is extended to include accurate originator information and other related messages made via electronic fund transfers. The Government of Samoa (GOS) has made progress in developing its anti-money laundering/counterterrorist finance regime in 2007 by enacting the Money Laundering Prevention Act. The GOS should ensure that financial institutions submit suspicious transaction reports (STRs) to the FIU and that the FIU forwards any STR worthy of investigation to law enforcement for possible prosecution. The GOS should effectively regulate its offshore financial sector by ensuring that the names of the actual beneficial owners of international business companies and banks are on a registry accessible to law enforcement. The GOS should ensure that the UNSCR 1267 Sanctions Committee Consolidated and U.S. lists are circulated and an effective asset forfeiture regime is established and implemented. The GOS should adhere to the Financial Action Task Force's 9 Special Recommendations on Terrorist Financing. In particular, Samoa should take steps to implement Special Recommendation IX on cash couriers and ensure that its entry and exit points are not used for either the transshipment of narcotics, the sale of imported narcotics, or the funds derived from either illicit activity.

Saudi Arabia

The Kingdom of Saudi Arabia is a growing financial center in the Gulf Region of the Middle East. However, there is no indication that narcotics-related money laundering currently is vulnerability in the country. Saudi Arabia is neither a major center within the region for financial crimes nor an offshore financial center. Saudi officials acknowledge difficulty in following the money trail due to the preference for cash transactions in the country. Money laundering and terrorist financing are known to originate from Saudi criminal enterprises, private individuals, and Saudi-based charities. There is an absence of official criminal statistics, but reportedly, there was no significant increase in financial crimes during 2008. It is believed the proceeds of crime from stolen cars and counterfeit goods are substantial. All eleven commercial banks in Saudi Arabia operate as standard "Western-style" financial institutions and are under the supervision of the central bank, the Saudi Arabian Monetary Agency (SAMA). In 2003, Saudi Arabia approved a new Anti-Money Laundering Law that contains criminal penalties for money laundering and terrorist financing. The law bans conducting commercial or financial transactions with persons or entities using pseudonyms or acting anonymously; requires financial institutions to maintain records of transactions for a minimum of ten years; adopts precautionary measures to uncover and prevent money laundering operations; requires banks and financial institutions to report suspicious transactions; authorizes government prosecutors to investigate money laundering and terrorist financing; and, allows for the exchange of information and judicial actions against money laundering operations with countries with which Saudi Arabia has official agreements.

In May 2003, SAMA issued updated anti-money laundering and counterterrorist finance guidelines for the Saudi banking system in accordance with the Financial Action Task Force's (FATF) 40 Recommendations on Money Laundering and the Nine Special Recommendations on Terrorist Financing. The guidelines require that banks have mechanisms to monitor all types of "Specially Designated Nationals" as listed by SAMA; that fund transfer systems be capable of detecting specially designated nationals; that banks strictly adhere to SAMA circulars on opening accounts and dealing with charity and donation collection; and that banks be able to provide the remitter's identifying information for all outgoing transfers. The guidelines also require banks to use software to profile customers to detect unusual transaction patterns; establish a monitoring threshold of 100,000 Saudi Riyals (approximately $26,700) and develop internal control systems and compliance systems. SAMA also issued "know- your-customer" guidelines, requiring banks to freeze accounts of customers who do not provide updated account information. Saudi law prohibits nonresident individuals or corporations from opening bank accounts in Saudi Arabia without the specific authorization of SAMA. There are no bank secrecy laws that prevent financial institutions from reporting client and ownership information to bank supervisors and law enforcement authorities. There is money laundering training for bank employees, prosecutors, judges, customs officers and other government officials. Financial institutions in Saudi Arabia are required to maintain records of significant transactions in order to respond quickly to government requests. Anti-money laundering and countering the financing of terrorism (AML/CTF) controls are applied to nonbank financial institutions and designated nonfinancial businesses and professions.

In 2005, the Government of Saudi Arabia (GOSA) established the Saudi Arabia Financial Investigation Unit (SAFIU), which acts as the country's financial intelligence unit (FIU) within the Ministry of Interior. Saudi banks are required to have anti-money laundering units with specialized staff to work with SAMA, the SAFIU and law enforcement authorities. All banks are also required to file suspicious transaction reports (STRs) with the SAFIU. The SAFIU collects and analyzes STRs and other available information and makes referrals to the Bureau of Investigation and Prosecution, the Mabahith (the Saudi Security Service), and the Public Security Agency for further investigation and prosecution.

The FIU performs analytical duties relating to financial crimes and also has law-enforcement and regulatory responsibilities. The FIU has access to databases of other government and financial institution entities. Statistics for suspicious transaction reporting and other forms of financial intelligence are not available. The SAFIU is not a member of the Egmont Group.

Hawala and money service businesses outside banks and licensed money changers are illegal in Saudi Arabia. Some instances of money laundering and terrorist finance in Saudi Arabia have involved hawala. To help counteract the appeal of hawala, particularly to many of the approximately six million expatriates living in Saudi Arabia, Saudi banks have taken the initiative to create fast, efficient, high quality, and cost-effective fund transfer systems that have proven capable of attracting customers accustomed to using hawala. An important advantage for the authorities in combating potential money laundering and terrorist financing in this system is that the senders and recipients of fund transfers through this formal financial sector are required to clearly identify themselves. In 2005, in an effort to further regulate the more than $16 billion in annual remittances that leave Saudi Arabia, SAMA consolidated the eight largest moneychangers into a single bank, Bank Al-Bilad.

In June 2007 the GOSA enacted stricter regulations on the cross-border movement of money, precious metals, and jewels. Money and gold in excess of 60,000 Saudi riyals (approximately $16,000) must be declared upon entry and exit from the country using official Customs forms. However, the implementation and effectiveness of these procedures remains in question. Cash declarations as well as smuggling reports are entered into a database; however, this information currently is not shared with other governments.

The new 2007 regulations also stipulate that whoever is convicted of money laundering will be imprisoned for up to ten years and fined up to five million Saudi riyals (approximately $1,333,300). The regulations also state, "Whoever funds terrorists or terror organizations is considered to be committing a crime of money laundering."

Saudi individual donors and unregulated charities have been a major source of financing to extremist and terrorist groups over the past 25 years. However, the Final Report of the National Commission on Terrorist Attacks Upon the United States, known as The 9/11 Commission, found no evidence that either the Saudi Government, as an institution, or senior Saudi Government officials individually, funded al-Qaida.

Contributions to charities in Saudi Arabia usually consist of Zakat, which refers to an Islamic religious duty with specified humanitarian purposes. In 2002, Saudi Arabia announced its intention to establish a National Commission for Relief and Charitable Work Abroad, commonly known as the Charities Commission, a mechanism that would oversee all private charitable activities abroad. Until the Charities Commission is established, no Saudi charity can send funds abroad. As of late 2008, the proposal was still under review by a committee of Saudi officials; however, the GOSA stated that the Commission should be fully functional by the end of 2009. As required by regulations in effect for over 20 years, domestic charities in Saudi Arabia are licensed, registered, audited, and supervised by the Ministry of Social Affairs. In addition to domestic charities are larger Saudi-based entities referred to "multilateral organizations" that engage in a range of domestic and international charitable and educational activities. These organizations, such as the International Islamic Relief Organization and the World Assembly of Muslim Youth, largely operate outside of the strict Saudi restrictions covering domestic charities. The Ministry has engaged outside accounting firms to perform annual audits of charities' financial records and has established an electronic database to track the operations of such charities. New banking rules implemented in 2003 that apply to all charities include stipulations that they can be only opened in Saudi riyals; must adhere to enhanced identification requirements; must utilize one main consolidated account; and must make payments only by checks payable to the first beneficiary, which then must be deposited in a Saudi bank. Regulations also forbid charities from using ATM and credit cards for charitable purposes, from making cash contributions, and making money transfers outside of Saudi Arabia.

In June 2008 the U.S. Department of the Treasury designated the Al Haramain Islamic Foundation (AHF), including its headquarters in Saudi Arabia, for having provided financial and material support to al-Qaida. Previously, the GOSA joined the United States in designating several branch offices of AHF and, due to actions by Saudi authorities, AHF had largely been precluded from operating in its own name. Despite these efforts, AHF leadership attempted to reconstitute the operations of the organization, and parts of the organization continued to operate. AHF is one of the world's largest Wahhabi affiliated Islamic charities. AHG has long been aligned with many of the activities of the Muslim Brotherhood, with chapters in Western Europe, the Balkans, the United States, and Canada.

SAMA is responsible for the tracing, freezing, and seizing of assets related to financial crimes. The banking community cooperates with SAMA regarding the tracing of funds as well as seizing and freezing of bank accounts. Existing laws on asset seizure and forfeiture are enforced by SAMA; however, there are currently no laws that allow the sharing of seized assets with other governments. The GOSA has been partially complaint with obligations under UN Security Council resolutions (UNSCR) on terrorist financing. SAMA circulates to all financial institutions under its supervision the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list.

There are no free trade zones for manufacturing, although there are bonded transit areas for the trans-shipment of goods not entering the country.

Saudi Arabia participates in the activities of the FATF through its membership in the Gulf Cooperation Council (GCC), and as a member of the Middle East and North Africa Financial Action Task Force (MENAFATF). Saudi Arabia will be undergoing a second FATF mutual evaluation in February 2009. Saudi Arabia is a party the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention for the Suppression of the Financing of Terrorism. Saudi Arabia has signed but not ratified the UN Convention against Corruption.

The Government of Saudi Arabia is taking steps towards enforcing its anti-money laundering/counterterrorist finance laws, regulations, and guidelines. However, Saudi Arabia continues to be a significant jurisdictional source for terrorist financing worldwide. The GOSA continues to take aggressive action to target direct threats to the Kingdom, but could do more to target Saudi-based support for extremism outside of Saudi's borders. Saudi authorities should hold terrorist financiers publicly accountable through prosecutions and full implementation of UNSC obligations. The GOSA also needs to take concrete steps to establish a charities oversight mechanism that also overseas "multilateral organizations" and enhances its oversight and control of Saudi entities with overseas operations. Charitable donations in the form of gold, precious stones and other gifts should be scrutinized. There is still an over-reliance on suspicious transaction reporting to generate money laundering investigations. Law enforcement agencies should take the initiative and proactively generate leads and investigations, and be able to follow the financial trails wherever they lead. The public dissemination of statistics regarding predicate offenses and money laundering prosecutions would facilitate the evaluation and design of enhancements to the judicial aspects of its AML system. Saudi Arabia should become a party to the UN Convention against Corruption.

Senegal

A regional financial center with a largely cash-based economy, Senegal is vulnerable to money laundering. Reportedly, most money laundering involves domestically generated proceeds from corruption and embezzlement. In 2008, authorities discovered significant amounts of irregular and inappropriate budget expenditure. Also of concern are criminal figures who launder and invest their personal and their organization's proceeds from the growing West Africa narcotics trade. There is also evidence of increasing criminal activity by foreigners, such as narcotics trafficking by Latin American groups and trafficking in persons involving Pakistanis.

Dakar's active real estate market is largely financed by cash. Property ownership and transfer are not transparent. The building boom and high property prices suggest that there is an increasing amount of funds with uncertain origin circulating in Senegal. The growing presence of hawala or other informal cash transfer networks and the increasing number of used imported vehicles also suggest the existence of both money laundering and illicit cash couriers. Trade-based money laundering (TBML) is centered in the region of Touba, a largely autonomous and unregulated free-trade zone under the jurisdiction of the Mouride religious authority. Touba reportedly receives between $550 and $800 million per year in funds repatriated by networks of Senegalese traders and vendors abroad. Other areas of concern include the transportation of cash, gold and gems through Senegal's airport and across its porous borders, and real estate investment in the Petite Cote south of Dakar.

Seventeen commercial banks operate alongside thriving micro credit and informal sectors. The Government of Senegal (GOS) is attempting to discourage its civil servants from using cash by depositing salaries into formal bank accounts, and the Banking Association has undertaken a publicity campaign to encourage the populace to use the formal banking system. Western Union, Money Gram and Money Express are associated with banks and compete with Senegal's widespread informal remittance systems, including hawala networks and cash couriers. Small-scale, unregulated and unlicensed currency exchange operations are common, especially outside urban centers. The Banque de l'Habitat du Senegal (BHS), a Senegalese bank, has affiliates licensed as money remitters in the

United States. New York State authorities have brought enforcement action against BHS New York for failing to comply with anti-money laundering (AML) regulations.

The Central Bank of West African States (BCEAO), based in Dakar, is the Central Bank for the eight countries in the West African Economic and Monetary Union (WAEMU or l'UEMOA), including Senegal, and uses the CFA franc currency. The Commission Bancaire (CB), the BCEAO division responsible for bank inspections, is based in Abidjan. The CB supervises and regulates banks within the WAEMU, but does not execute a full AML examination during its standard banking compliance examinations. Senegal has no offshore banking sector.

Senegal's currency control and reporting requirements are not uniform and are reportedly laxly enforced. Nonresidents on entry must declare any currency they are transporting from outside the "zone franc" greater than one million CFA (approximately $2,000). They must also declare monetary instruments denominated in cash in any amount. When departing Senegal, nonresidents must declare any currency from outside the franc zone greater than approximately $1,000 and all monetary instruments from foreign entities. The law does not require residents to declare currency on entry; on exit, they must declare amounts any foreign currency and any monetary instruments greater than approximately $4,000. All declarations must be in writing. There is no publicity regarding currency declaration requirements at major points of entry. Customs authorities are primarily concerned with the importation of dutiable goods. Other authorities with different mandates, and which do not implement currency controls, patrol land border crossings

The legal basis for Senegal's anti-money laundering/counterterrorist financing (AML/CTF) framework is "la Loi Uniforme Relative a la Lutte Contre le Blanchiment de Capitaux" No. 2004-09 of February 6, 2004, or the Anti-Money Laundering Uniform Law (Uniform Law). As the common law passed by the members of l'UEMOA/WAEMU, all member states are bound to enact and implement the legislation. Among the union, Senegal was the first country to have the AML legal framework in place. Senegal has an "all crimes" approach to money laundering. Self launderers may be prosecuted and the law does not require a conviction for the predicate offense. Intent may be inferred from objective factual circumstances. Criminal liability applies to all legal persons as well as natural persons.

The legislation lacks certain compliance provisions for nonfinancial institutions. The Uniform AML law requires banks and other financial institutions to know their customers and record and report the identity of any individual or entity engaged in significant transactions, including the recording of large currency transactions. Banks monitor and record the origin of any deposit higher than 5 million CFA (approximately $10,000) for a single individual account and 20 to 50 million CFA (approximately $40,000 to 100,000) for any business account. Commercial banks in Senegal are improving their internal controls and enhancing their "know your customer" (KYC) requirements. The law also contains safe harbor provisions for individuals who file reports.

Cellule Nationale de Traitement des Informations Financieres (CENTIF), Senegal's financial intelligence unit (FIU) became operational in August 2005. The FIU currently has a staff of 28, including six appointed members: the President of the FIU, who by law is chosen from the Ministry of Economy and Finance, and five others detailed from the Customs Service, the BCEAO, the Judicial Police, and the Ministry of Justice. Senegal's FIU is working to improve its operational abilities and raise the awareness of the threat of money laundering in Senegal. CENTIF has provided outreach and training for obliged entities to familiarize themselves with the legal requirements and to improve the quality and variety of STRs that the FIU receives. Senegal's FIU has applied for membership in the Egmont Group.

The police, gendarmerie and Ministry of Justice's judicial police are technically responsible for investigating money laundering and terrorist financing. However, in reality, CENTIF reportedly retains its information and tasks law enforcement entities to investigate or retrieve information for its

cases. CENTIF reportedly does not share or disseminate information or financial intelligence to law enforcement. In 2008, CENTIF received 58 suspicious transaction reports (STRs), mostly from banks, and referred 30 cases, which include transactions from both Senegalese and foreigners, to the Prosecutor General. In turn, the Prosecutor General passed 10 cases directly to the investigating judge. No cases have been concluded, although authorities have made commitments to pursue judicial actions. Official statistics regarding the prosecution of financial crimes are unavailable. There has been only one known conviction for money laundering since 2005, which led to the confiscation of a private villa.

The Uniform Law provides for the freezing, seizing, and confiscation of property by judicial order. In addition, the FIU can order the suspension of the execution of a financial transaction for 48 hours. The BCEAO can also order the freezing of funds held by banks. The Uniform Law allows explicitly for criminal forfeiture. There is no provision for civil forfeiture. The FATF-style regional body (FSRB) for the 15 members of the Economic Community of Western African States (ECOWAS) known as the Intergovernmental Action Group Against Money Laundering in West Africa (GIABA) has also drafted a uniform law regarding seizure and confiscation, which it hopes that all of its member states will enact.

The BCEAO has released a Directive against Terrorist Financing that advises member states that they must enact a law against terrorist financing; the BCEAO law is a Uniform Law to be adopted by all WAEMU/l'UEMOA members in a manner similar to that of the AML law. Like the AML law, the terrorist financing law is a penal law, and each national assembly must enact enabling legislation to adopt it. In 2008, Senegal's Council of Ministers approved this l'UEMOA/WAEMU CTF uniform law, and it currently awaits adoption by the National Assembly. Reportedly, when the law is placed on the agenda, it should pass quickly; however, the Assembly has not yet put it on the agenda. The CENTIF hoped to have the law passed prior to its February presentation to the Egmont Group regarding its application for membership.

Although Senegal has not passed a law criminalizing the financing of terrorism, it amended its penal code in March 2007 to incorporate the United National Security Council Resolution (UNSCR) requirements for terrorist financing. In July 2007, l'UEMOA/WAEMU released guidance on terrorist financing for the sub-region alongside Directive No. 04/2007/CM/l'UEMOA, obliging member states to pass domestic CTF legislation. The BCEAO and the FIU circulate the UN 1267 Sanctions Committee consolidated list to commercial financial institutions. To date, Senegalese authorities have not identified any designated entities. The l'UEMOA/WAEMU Council of Ministers issued a directive in September 2002 requiring banks to freeze the assets of any entities designated by the Sanctions Committee.

Senegal has entered into bilateral criminal mutual assistance agreements with France, Tunisia, Morocco, Mali, The Gambia, Guinea Bissau, and Cape Verde. Multilateral ECOWAS treaties address extradition and legal assistance among the member countries. Under the Uniform Law, the FIU may share information freely with other l'UEMOA/WAEMU FIUs. All WAEMUs countries have FIUs, except Guinea Bissau. CENTIF has signed a Memorandum of Understanding (MOU) for information exchange with the FIUs of Belgium, Nigeria, Algeria and Lebanon, and is working on other accords. CENTIF is open to information exchange on the basis of reciprocity and shares information with the FIUs belonging to the Egmont Group without the requirement of a MOU. The Senegalese government and law enforcement agencies are generally willing to cooperate with United States law enforcement agencies. The Government of Senegal (GOS) has also worked on international anti-crime operations with INTERPOL, Spanish, and Italian authorities.

Senegal is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the 1999 UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Corruption. Senegal is a member of GIABA and underwent

a mutual evaluation by that body. GIABA discussed and adopted the mutual evaluation report in May 2008.

The Government of Senegal should continue to work with its partners in GIABA, l'UEMOA/WAEMU and ECOWAS to develop a comprehensive anti-money laundering and counterterrorist financing regime. Senegal should work on achieving transparency in its financial and real estate sectors, and continue to encourage the populace to use the formal banking system, steering them away from cash transactions. Senegal should continue to battle corruption and increase the frequency, transparency, and effectiveness of financial reviews and audits of financial institutions. Senegal should lead its regional partners in the fight against AML/CTF and establish better uniform control of cross-border flow of currency and other bearer-negotiable instruments for both residents and nonresidents. Senegalese law enforcement and customs authorities need to develop their expertise in identifying and investigating both traditional money laundering and money laundering within the informal economy. CENTIF should perform more outreach to obliged nonbank financial institutions to ensure a better understanding of STRs, when to file them and the information they should contain. CENTIF, law enforcement and Ministry of Justice authorities should work together to coordinate roles and responsibilities with regard to case investigation and assembly, and develop a deeper interagency understanding of money laundering and terrorist financing. Senegal should amend its AML legislation to address the remaining shortcomings, and criminalize terrorist financing.

Serbia

Serbia is not a regional financial center. At the crossroads of Europe and on the major trade corridor known as the "Balkan route," Serbia confronts narcotics-trafficking, smuggling of persons, drugs, weapons and pirated goods, money laundering, and other criminal activities. Corruption and organized crime also continue to be significant problems in Serbia. Serbia continues to be a significant black market for smuggled goods. Illegal proceeds are generated from drug-trafficking, corruption, tax evasion and organized crime, as well as other types of crimes. Proceeds from illegal activities are invested in all forms of real estate. Trade-based money laundering, in the form of over- and under-invoicing, is commonly used to launder money. There are reports the purchase of some private and state-owned companies was linked to money laundering activity.

A significant volume of money flows to Cyprus, reportedly as payment for goods and services. The records maintained by various government entities vary significantly on the volume and value of imports from Cyprus. According to Government of the Republic of Serbia (GOS) officials, much of the difference is due to payments made to accounts in Cyprus for goods, such as Russian oil, that actually originate in a third jurisdiction. Banks in Macedonia, Hungary, Switzerland, Austria and China have emerged as destinations for laundered funds.

There are 34 banks in Serbia. Twenty are foreign majority owned, six are majority owned by domestic legal entities and eight are state majority owned. Foreign majority ownership accounts for approximately 75 percent of total bank assets in Serbia. There is no provision in the banking law that allows the establishment of offshore banks, shell companies or trusts. Reportedly, there is no official evidence of any alternative remittance systems operating in the country; however, there is anecdotal evidence. Nor is there evidence of financial institutions engaging in currency transactions involving international narcotics-trafficking proceeds. Serbia has three designated, operating free trade zones established to attract investment by providing tax-free areas to companies. These companies are subject to the same supervision as other businesses in the country.

In September 2005, Serbia codified an expanded definition of money laundering in Article 231 of the Penal Code. This legislation gives police and prosecutors more flexibility to pursue money laundering charges, as the law broadens the scope of money laundering and aims to conform to international standards. The penalty for money laundering is a maximum of ten years imprisonment. Under this law

and attendant procedure, money laundering falls into the serious crime category and permits the use of Mutual Legal Assistance (MLA) procedures to obtain information from abroad.

On November 28, 2005, Serbia adopted a revised anti-money laundering law (AMLL), replacing the July 2002 Law on the Prevention of Money Laundering. The revised AMLL expands the number of entities required to collect certain information and file currency transaction reports (CTRs) with the financial intelligence unit (FIU) for all cash transactions over EUR 15,000 (approximately $20,250), or the dinar equivalent. Suspicious transactions in any amount must be reported to the FIU. The law also expands those sectors subject to reporting and record keeping requirements. Banks, attorneys, auditors, tax advisors and accountants, currency exchanges, insurance companies, casinos, securities brokers, dealers in high value goods, real estate agencies and travel agents are required to comply with the AMLL provisions. Required records must be maintained for five years. These entities are protected with respect to their cooperation with law enforcement entities. In addition to reporting to the FIU, the AMLL also requires obligated entities and individuals to monitor customers' accounts when they suspect money laundering. The AMLL also eliminates a previous provision limiting prosecution to crimes committed within Serbian territory

The Law on Foreign Exchange Operations, adopted in 2006, criminalizes the use of false or inflated invoices or documents to facilitate the transfer of funds out of the country. This law was enacted in part to counter the perceived problem of import-export fraud and trade-based money laundering. According to the law, residents and nonresidents are obliged to declare to customs authorities all currency (foreign or dinars), or securities in amounts exceeding EUR 5,000 (approximately $6,750) being transported across the border.

Among the pending legislative initiatives necessary for Serbia to be fully compliant with international standards is the GOS Anti Money Laundering and Terrorism Financing Bill, extending financial reporting requirements to terrorist financing and expanding all current AMLL requirements to nonbank financial institutions. In September 2008, the GOS proposed this bill to the Parliament.

In September 2008, the GOS adopted the National Strategy Against Money Laundering and Terrorist Financing. The Strategy sets out specific goals and objectives in legislation, operational matters and training.

In October 2008, the Parliament enacted a new Anti-Corruption Agency Law that, among other provisions, establishes an anticorruption agency and sets reporting and political party funding requirements. At the same time, it also enacted the Law on the Amendments and the Addenda of the Law on Financing Political Parties, improving the reporting obligations and procedure.

Also in October 2008, the Parliament of Serbia adopted the Law on Criminal Liability of Legal Entities, providing for criminal liability of legal persons for money laundering and terrorist financing.

The National Bank of Serbia (NBS) has supervisory authority over banks, currency exchanges, insurance and leasing companies. The NBS has issued regulations requiring banks to have compliance and know-your-customer (KYC) programs in place and to identify the beneficial owners of new accounts. In June 2006, the NBS expanded its customer identification and record keeping rules by adopting new regulations mandating enhanced due diligence procedures for certain high risk customers and politically exposed persons. Similar regulations have been adopted for insurance companies. The Law on Banks includes a provision allowing the NBS to revoke a bank's license for activities related to, among other things, money laundering and terrorist financing. To date, the NBS has not used this revocation authority. The legal framework is in place, but the NBS is still building the capacities needed for effective anti-money laundering (AML) compliance supervision through training and staff development.

The Securities Commission (SC) supervises broker-dealers and investment funds. The Law on Investment Funds and the Law on Securities and Other Financial Instruments Market, both enacted in

2006, provide the SC with the authority to "examine" the source of investment capital during licensing procedures. The SC is also charged with monitoring its obligors' compliance with the AML laws. Regulations to implement this authority are being developed.

In 2004, a new law was enacted that revises gaming rules, and the Administration for Games of Chance was established on January 1, 2005. The law rescinds all outstanding gaming establishment licenses and requires existing casinos to reapply for new licenses. It also sets a maximum of ten casino licenses for issuance. As of the end of 2008, only two casinos had been issued new licenses. Yet, casinos continue to operate all over the country in apparent violation of the new law. The gaming supervisory authority has not been provided with adequate resources (five of the ten authorized staff), and the political will to enforce the law is weak.

Since the GOS introduced a value-added tax (VAT) in 2005, several criminal schemes have been investigated. Serbia's Tax Administration lacks the audit and investigative capacity and resources to adequately investigate the large number of suspicious transactions that are forwarded by Serbia's FIU. In addition, current tax law sets a low threshold for auditing purposes and has increased the burden on the Tax Administration. This creates a situation where criminals can spend and invest illegal proceeds freely with little fear of challenge by the tax authorities or other law enforcement agencies.

The Administration for the Prevention of Money Laundering serves as Serbia's FIU with the status of an administrative body under the Ministry of Finance. The FIU has its own line item operating budget. The FIU has filled 24 of its 35 authorized positions. In accordance with the AMLL, the FIU developed listings of suspicious activity red flags for banks, currency exchange offices, insurance companies, securities brokers and leasing companies. The FIU has the authority to freeze transactions for a maximum of 72 hours and to order the monitoring of an account for up to three months following a freezing order. The FIU has signed memoranda of understanding (MOU) on the exchange of information with the NBS, Customs and the Tax Administration.

The FIU received 2,034 suspicious transaction reports (STRs) in 2007 and 2,087 through November 5, 2008. Virtually all of the STRs received by the FIU have been filed by commercial banks. Currency exchange offices have filed only seven STRs, all prior to 2004. The FIU opened 46 cases in 2007 and 31 through November 5, 2008. Prosecutors' offices have assigned AML liaison officers to ensure information sharing with the FIU.

A total of six criminal charges were submitted for money laundering violations in 2007. In late 2008, the public prosecutor's office reports 66 persons suspected of money laundering, with 33 requests for investigation and 27 issued and pending indictments. To date, there have been three convictions. In October 2008, Serbian police arrested an organized group of 25 people who are suspected of laundering money through phantom and unregistered companies. The group is suspected to have earned over 3 million euro (approximately $4,050,000) in money laundering operations over the last two years.

Despite its attempts to gain law enforcement authority, Serbian Customs has not succeeded in doing this to date. Although Customs has investigative and intelligence functions, investigations for all cases to be prosecuted are turned over to the MOI. In addition, Serbian capability to monitor Danube traffic remains minimal.

The difficulty of convicting a suspect of money laundering without a conviction for the predicate crime and the unwillingness of the courts to accept circumstantial evidence to support money laundering or tax evasion charges is hampering law enforcement and prosecutors in following the movement and investment of illegal proceeds and effectively using the AML laws. The most common predicate crime is "abuse of office." The Suppression of Organized Crime Service (SOCS) of the Ministry of Interior houses an Anti-Money Laundering Section to better focus financial investigations.

In August 2005, the GOS established the Permanent Coordinating Group (PCG), an interagency working group originally tasked with developing a plan to implement the recommendations of the Financial Action Task Force-style regional body MONEYVAL's second-round evaluation conducted in October 2003. The PCG includes representatives from the FIU, Tax Administration, Customs Authority, Ministries of Interior and Justice, the Supreme Court, State Prosecutor's Office, the Securities Commission, and the NBS. Subgroups have been tasked with drafting amendments to the AMLL and with estimating the budget necessary to effectively implement the proposed new anti-money laundering/counterterrorist financing law when it is enacted. The PCG and the working groups meet intermittently as required for completing specific tasks. Most recently, the group has been meeting to develop guidance for supervisory bodies and financial institutions to help them implement a risk-based approach to anti-money laundering/counterterrorist financing. The government still needs better, more consistent interagency coordination to improve information sharing, record keeping and statistics.

In October 2008, the Parliament adopted its first ever Asset Forfeiture Law, stipulating the agencies in charge of detection of the proceeds of crime, process of seizure and the management of seized assets. This law also changes the burden of proof, making a convicted criminal be responsible for proving the legal origin of his assets. It also provides for international cooperation. Under the law, assets derived from criminal activity or suspected of involvement in terrorist financing can be seized upon conviction for an offense. The law defines the conditions, procedure and management of the seized criminal proceeds.

The FIU is charged with enforcing the UNSCR 1267 provisions regarding suspected terrorist lists. A draft law on terrorist financing, now pending Parliamentary approval, will apply all provisions of the AMLL to terrorist financing, require reporting to the FIU of transactions suspected to be terrorist financing and will create mechanisms for freezing, seizing and confiscation of suspected terrorist assets based on UNSCR provisions. Although the FIU routinely provides the UN list of suspected terrorist organizations to the banking community, examinations for suspect accounts have revealed no evidence of terrorist financing within the banking system. The SOCS, the Special Anti-Terrorist Unit (SAJ), and Gendarmerie, in the Ministry of Interior, are the law enforcement bodies responsible for planning and conducting the most complex anti-terrorism operations. SOCS cooperates and shares information with its counterpart agencies in countries bordering Serbia. Although Serbia has criminalized terrorist financing, the freezing, seizing and confiscation of terrorists' assets in accordance with UN Security Council resolutions still lacks a legal basis, pending enactment of the draft legislation.

Serbia has no laws governing its cooperation with other governments related to narcotics, terrorism, or terrorist financing. Bases for cooperation include participation in Interpol, bilateral and multi-lateral cooperation agreements, and agreements concerning international legal assistance. There are no laws governing the sharing of confiscated assets with other countries, nor is any legislation under consideration.

Serbia does not have a mutual legal assistance arrangement with the United States, but information exchange via a letter rogatory is standard. The 1902 extradition treaty between the Republic of Serbia and the United States remains in force. The treaty allows the Serbian government to extradite non-Serbs to the United States. The GOS has bilateral agreements on mutual legal assistance with 31 countries. The GOS is an active member of MONEYVAL, and Serbia is scheduled for a mutual evaluation by MONEYVAL in 2009. The FIU is a member of the Egmont Group and actively participates in information exchanges with counterpart FIUs, including FinCEN. The Serbian FIU has also signed information sharing MOUs with Macedonia, Romania, Belgium, Slovenia, Montenegro, Albania, Georgia, Ukraine, Bulgaria, Croatia, and Bosnia and Herzegovina. Serbia is a party to the1988 UN Drug Convention, the UN Convention against Corruption and the UN Convention against Transnational Organized Crime. The GOS also is a party to the UN Convention for the Suppression of

the Financing of Terrorism, although domestic implementation procedures do not provide the framework for full application.

The Government of Serbia should continue to work toward eliminating the abuses of office and culture of corruption that enable money laundering and financial crimes. The Parliament of Serbia should enact its pending legislative initiatives, including the Government Bill on Anti Money Laundering and Terrorism Financing, extending financial reporting requirements to suspected terrorist financing. The GOS should adopt regulations and bylaws to implement all reporting and record keeping requirements of the current AMLL applicable to covered nonbank financial institutions. The GOS should enforce regulations pertaining to money service businesses and obligated nonfinancial businesses and professions. The supervisory scheme should be completed, and implementing regulations should be binding for the securities sector. The National Bank and other supervisory bodies as well as investigative agencies, prosecutors and judges need enhanced capability and additional resources. The gaming laws should be fully enforced and the supervisory authority provided with adequate resources and authority. Rather than address specific tasks as an ad hoc group, the PCG should meet on a regular basis to discuss issues and projects, and work to improve interagency coordination in such areas as information sharing, record keeping and statistics. Serbia should take steps to ensure Customs has the authority and resources to investigate pertinent cases leading to prosecutions and to effectively police its Danube border.

Seychelles

Seychelles is a not a major financial center. The existence of a developed offshore financial sector, however, makes the country vulnerable to money laundering. The Government of Seychelles (GOS), in efforts to diversify its economy beyond tourism, developed an offshore financial sector to increase foreign exchange earnings and actively markets itself as an offshore financial and business center that allows the registration of nonresident companies. As of January 2008, there were 43,456 registered international business companies (IBCs) and 211 trusts that pay no taxes in Seychelles, and are not subject to foreign exchange controls. The Seychelles International Business Authority (SIBA), a body with board members from both the government and the private sector, registers, licenses and regulates offshore activities. The SIBA licenses and registers agents who carry out due diligence tests when registering new companies in the Seychelles offshore sector. The SIBA also regulates the activities, which are mainly geared towards exports, of the Seychelles International Trade Zone,

In addition to IBCs and trusts, Seychelles permits offshore insurance companies, mutual funds, and offshore banking. In November 2006, under the Mutual Funds Act, the Securities Act and the Insurance Act, the GOS established the Non-Bank Financial Services Authority to regulate these sectors. Three offshore insurance companies have been licensed: one for captive insurance and two for general insurance. Seychelles has two offshore banks: Barclays Bank (Offshore Unit) and BMI Offshore Bank. BMI Offshore Bank is a joint venture between the Bahrain-based BMI Bank and the locally incorporated Nouvobanq, the largest bank in Seychelles. The International Corporate Service Providers Act 2003, designed to regulate all activities of corporate and trustee service providers, entered into force in 2004.

In its 2007-2017 Strategic Plan, the Seychelles Government proposes to facilitate the development of the financial services sector as a third pillar of the economy. It plans to achieve this through actively promoting Seychelles as an internationally recognized offshore jurisdiction, with emphasis on IBCs, mutual funds, special license companies and insurance companies.

In an attempt to build on the success of the financial services sector and to maintain investors' confidence, the 1995 Securities Act and the 1997 Mutual Funds Act were amended in 2007 and 2008 respectively. The 2007 Securities Act aims at instilling confidence in investors by licensing and regulating all securities-related activities and by providing internationally accepted guidelines to which

participants must adhere. The Act establishes fines against insider trading, price rigging, market manipulation, and fraudulent transactions. The Act also establishes the Seychelles Stock Exchange, which will be regulated by the Securities and Financial Markets Division of the Central Bank. The 2008 Mutual and Hedge Funds Act extends the authorities' power to obtain periodical audits, enter and search premises of licensed operators, and ensure that activities conform to international standards.

In June 2008, the Central Bank of Seychelles issued guidelines (The Fit and Proper Guidelines) outlining relevant licensing criteria under the Securities Act, the Insurance Act and the Mutual Funds Act.

In 1996, the GOS enacted the Anti-Money Laundering Act (AMLA), which criminalized the laundering of funds from all serious crimes, required covered financial institutions and individuals to report suspicious transactions to the Central Bank, which now houses the financial intelligence unit (FIU), and established safe harbor protection for individuals and institutions filing such reports. The AMLA also imposed record keeping and customer identification requirements for financial institutions, and provided for the forfeiture of the proceeds of crime.

In May 2006, the Anti-Money Laundering Act 2006 came into force. This legislation replaced the 1996 AMLA and addresses many of the deficiencies previously cited by a 2004 IMF assessment. The 2006 AMLA applies the same money laundering controls, including the obligation to submit suspicious transaction reports (STRs), to the same entities as the 1996 law, but also applies to nonbank financial institutions, such as exchange houses, stock brokerages, insurance agencies, lawyers, notaries, accountants, and estate agents. Offshore banks are specifically addressed by the 2006 AMLA. The gaming sector is also obliged to file STRs. Although Internet gaming is an obligated sector, no offshore casinos or Internet gaming sites are licensed to operate in Seychelles and the law does not explicitly state that offshore gaming is covered in an identical manner. The 2006 AMLA discusses record-keeping and institutional protocol requirements, sets a maximum delay of two working days to file an STR, criminalizes tipping off, and sets safe harbor provisions. The new law also requires reporting entities to take "reasonable measures" to ascertain the purpose of any transaction in excess of Seychelles rupees 100,000 (approximately U.S. $6,250), or, in the case of cash transactions, rupees 50,000 (approximately U.S. $3,125), and the origin and destination of the funds involved in the transaction. However, it leaves open exceptions for "an existing and regular business relationship with a person who has already produced satisfactory evidence of identity"; for "an occasional transaction under rupees 50,000" (approximately U.S. $3,125); and in other cases "as may be prescribed."

Under the 2006 AMLA, anyone who engages directly or indirectly in a transaction involving money or other property (or who receives, possesses, conceals, disposes of, or brings into Seychelles any money or property) associated with a crime, knowing or having reasonable grounds to know that the money or property is derived from an illegal activity, is guilty of money laundering. In addition, anyone who aids, abets, procures, or conspires with another person to commit the crime, while knowing, or having reasonable grounds for knowing that the money was derived from an illegal activity, is likewise guilty of money laundering. Money laundering is sanctioned by imprisonment for up to fifteen years and/or rupees 3,000,000 (approximately U.S. $375,000) in penalties. Of 68 investigations to date, eleven were closed due to lack of evidence. In three cases, the suspects had left Seychelles, and in three others the suspects had died. The remaining 51 cases were still pending investigation as of December 2008. There have been no arrests or prosecutions for money laundering or terrorist financing since 1998.

In July 2008, the Anti-Money Laundering (Amendment) Bill was introduced in the National Assembly. The proposed amendment provides for an expanded definition of the crime of money laundering, which provides for offenses committed outside of Seychelles. It also provides for a civil standard of proof to determine the connection between the predicate offense and the money laundering

offense. In specified circumstances, the suspect must prove that assets were obtained legally; otherwise, authorities will presume the assets were derived from criminal conduct.

The Financial Institutions Act of 2004 imposes more stringent rules on banking operations and brings the Seychelles' regulatory framework closer to compliance with international standards. The law aims to ensure greater transparency in financial transactions by regulating the financial activities of both domestic and offshore banks. Among other provisions, the law requires that banks change their auditors every five years. Auditors must notify the Central Bank if they uncover criminal activity such as money laundering in the course of an audit. There is no cross-border currency-reporting requirement.

The Financial Intelligence Unit (FIU) was established within the Central Bank of Seychelles under Section 16 of the 2006 AMLA. The FIU is the focal point for receiving and analyzing reports of transactions suspected to be related to money laundering or the financing of terrorism, and disseminating the analysis to the appropriate law enforcement and supervisory agencies in Seychelles. To support these core functions, the FIU is authorized to collect pertinent information and request additional information from reporting entities, law enforcement and supervisory bodies. The law provides for the FIU to have a proactive targeting section to research trends and developments in money laundering and terrorist financing. The FIU also performs examinations of the reporting entities and, in concert with regulators, issues guidance related to customer identification, identification of suspicious transactions, and record keeping and reporting obligations. In 2007 the FIU updated a set of guidelines on anti-money laundering/counterterrorist financing (AML/CTF), for the reporting entities in accordance with the requirements of the AMLA 2006. In December 2006, the Seychelles Government established a National Anti-Money Laundering Committee to better coordinate the efforts of the various law enforcement agencies in combating financial crimes. The Committee is chaired by the FIU, and comprises representatives of the Police, the Attorney General's Office, Customs, Immigration, the Seychelles Licensing Authority, and the Seychelles International Business Authority.

The FIU cannot freeze or confiscate property but may get a court order to effect an asset freeze. The courts have the authority to freeze or confiscate money or property. Judges in the Supreme Court have the authority to restrain a target from moving or disposing of his or her assets, and will do so if a law enforcement officer requests it and the Court is "satisfied that there are reasonable grounds" for doing so. The Court also has the authority to determine the length of time for the restraint order and, as needed, the disposition of assets. If the target violates the order, he or she becomes subject to financial penalties. Law enforcement may seize property subject to this order to prevent it from being disposed of or moved contrary to the order. The Court is also authorized to order the forfeiture of assets.

In 2004, the GOS enacted the Prevention of Terrorism Bill. The legislation specifically recognizes the government's authority to identify, freeze, and seize assets related to terrorist financing. The 2006 AMLA broadened the legal AML requirements, applying the law to suspected terrorist financing transactions. Assets used in the commission of a terrorist act can be seized and legitimate businesses can be seized if used to launder drug money, support terrorist activity, or support other criminal activities. Both civil and criminal forfeiture are allowed under current legislation.

The Mutual Assistance in Criminal Matters Act of 1995 empowers the Seychelles Central Authority to provide assistance to another jurisdiction in connection with a request to conduct searches and seizures relating to serious offenses under the law of the requesting state. The Prevention of Terrorism Act extends the authority of the GOS to include the freezing and seizing of terrorism-related assets upon the request of a foreign state. To date, no such assets have been identified, frozen, or seized.

Seychelles is a party to the 1988 UN Drug Convention, the UN Convention Against Corruption, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. Seychelles circulates to relevant authorities the updated lists of names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions

Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O. 13224.

The Government of Seychelles is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a Financial Action Task Force-style regional body. Seychelles underwent a mutual evaluation conducted by ESAAMLG in November 2006. This exercise entailed a review of Seychelles' AML/CTF regime and covered their legal, financial and law enforcement framework and implementation. The ESAAMLG plenary adopted the report at its August 2008 plenary session. Due to the delay in the report, and the number of changes that the Seychelles has undergone since 2006, the plenary agreed to allow Seychelles to attach a narrative of Seychelles' AML/CTF improvements since the on-site evaluation.

Seychelles should expand its anti-money laundering efforts by prohibiting bearer shares and clarifying its law regarding the complete identification of beneficial owners. The GOS should also amend the AMLA to state explicitly that all offshore activity is regulated in the same manner and to the same degree as onshore. Seychelles should continue to work with its FIU to ensure it has the training and resources needed for outreach, analysis and dissemination, and comports with the membership criteria of the Egmont Group of FIUs. The GOS should also consider codifying the ability to freeze assets rather than issuing restraining orders, and developing a currency-reporting requirement for border entry. Seychelles should participate more actively in ESAAMLG, and address the remaining shortcomings as outlined in the mutual evaluation report.

Sierra Leone

Sierra Leone has a cash-based economy and is not a regional financial center. Government of Sierra Leone (GOSL) officials hypothesize that money laundering activities are pervasive, particularly in the diamond sector. Although there have been some attempts at tighter regulation, monitoring, and enforcement, in some areas significant diamond smuggling still exists. Drug smuggling is also a problem in Sierra Leone, as evidenced by the seizure of a plane in July 2008, carrying cocaine worth $54 million at an airport outside Freetown. Real estate and car dealerships are also sectors vulnerable to money laundering activities. Loose oversight of financial institutions, weak regulations, pervasive corruption, and a widespread informal money-exchange and remittance system contribute to an atmosphere conducive to money laundering. Authorities attempted in 2008 to strengthen oversight and regulatory frameworks, including in the mushrooming financial sector,

The President signed the Anti-Money Laundering Act (AMLA) in July 2005. The AMLA incorporates international standards, mandating suspicious activity reporting, setting safe harbor provisions, requiring know your customer (KYC) procedures and identification of beneficial owner, as well as mandating five-year record-keeping. There is a currency reporting requirement for deposits larger than 25 million leones (approximately $8,330) and no minimum for suspicious transaction reporting. The law requires that international financial transfers over $10,000 go through formal financial institution channels. The AMLA calls for cross-border currency reporting requirements for cash or securities in excess of $10,000. The law designates the Governor of the Bank of Sierra Leone as the national Anti-Money Laundering Authority.

The AMLA applies to Sierra Leone's financial sector institutions, including depository and credit institutions, money transmission and remittance service businesses, insurance brokers, investment banks, securities and stock brokerage houses, and currency exchange houses. In 2008, the Bank of Sierra Leone held a stakeholder conference, which all local banks attended, to establish guidelines for money laundering prevention. The law is also applicable to designated nonfinancial businesses and professions such as casinos, realtors, dealers in precious metals and stones, notaries, legal practitioners, and accountants.

A financial intelligence unit (FIU) exists but lacks the capacity to effectively monitor and regulate financial institution operations. The FIU's role is to receive and analyze financial information and intelligence, including suspicious transaction reports (STRs), and disseminate information regarding potential cases to law enforcement agencies for investigation. The AMLA charges the Central Intelligence Security Unit (CISU) and the Attorney General's Office with investigating reports made by the FIU, but CISU cannot undertake a complete investigations or effect arrests. The Attorney General's Office has neither investigative nor arrest powers in its mandate. Though, in theory, the Sierra Leone Police (SLP), National Revenue Authority, or Anti-Corruption Commission could be tasked by either entity with investigating reported money laundering crimes, it is not clear if this happens in practice. Limited resources hamper law enforcement efforts in all arenas. Lack of training on this subject is also a considerable hindrance to prosecutions. No financial institutions provided a suspicious transaction report this year; nor have there been any prosecutions under the AMLA in 2008, The AMLA empowers the courts to freeze assets for seventy-two hours if a suspect has been charged with money laundering or if a charge is imminent. Upon a conviction for money laundering, all property is treated as illicit proceeds and can be forfeited unless the defendant can prove that possession of some or all of the property was obtained through legal means. The AMLA also provides the basis for mutual assistance and international cooperation.

Sierra Leone is a member of the Groupe Intergouvernemental d'Action contre le Blanchiment d'Argent en Afrique de l'Ouest (GIABA), a Financial Action Task Force-style regional body (FSRB) and is obliged to uphold and proliferate the AML/CTF standards instituted by that body. Sierra Leone's mutual evaluation was adopted by the GIABA plenary in June 2007. The evaluation, which was conducted by the World Bank on GIABA's behalf, noted particular areas of concern. These concerns included substantive shortcomings in the AMLA; the lack of implementation of the AMLA, in particular the failure to establish an operational FIU; limited financial sector supervision by the Bank of Sierra Leone (BSL) of AML/CTF preventive measures; and the lack of institutional mechanisms for the implementation of UNSCRs 1267 and 1373.

The GOSL is currently reviewing the AMLA with stakeholders, and has drafted an amended law for passage in 2009. The proposed revision includes provisions criminalizing the financing of terrorism. The revised law would also assign an appropriate law enforcement agency, such as the Sierra Leone Police (SLP), primary responsibility for money laundering and terrorism financing investigations, and increase the penalties for money laundering, The World Bank and GIABA have both provided input on the revision process to ensure that the law will meet international standards and guidelines.

Sierra Leone is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Sierra Leone is a party to the UN Convention against Corruption.

Although the Government of Sierra Leone is aware that attention and action are required in this area and has enacted anti-money laundering legislation, it remains to be effectively implemented. Proposed revisions to the law should correct deficiencies in the original act, and include provisions for combating the financing of terrorism. Authorities should ensure that the revised law is harmonized with other relevant legislation, including the revised Anti-Corruption Act (2008), National Drug Control Act (2008), and Anti-Terrorism Act. The GOSL should ensure its penalties for counterterrorist financing are significant. The GOSL should also ensure the regular distribution to financial institutions of the UNSCR 1267 Sanctions Committee's consolidated list, and implement and enforce provisions for immediate freezing of assets based on the list.

The GOSL should increase the level of awareness and understanding of money laundering issues and allocate the necessary human, technical, and financial resources to implement such a program. Sierra Leone's FIU should work to build capacity by increasing its resources and striving to organize itself

and perform according to international standards. Sierra Leone should continue its efforts to counter the smuggling of diamonds and narcotics, and regulate sectors in which money laundering is known or thought to be pervasive. Sierra Leone should continue to take steps to combat corruption at all levels of commerce and government. The GOSL needs to ratify the UN Convention against Transnational Organized Crime.

Singapore

As a significant international financial and investment center and, in particular, as a major offshore financial center, Singapore is vulnerable to money launderers. Stringent bank secrecy laws and the lack of routine currency reporting requirements make Singapore a potentially attractive destination for drug traffickers, transnational criminals, terrorist organizations and their supporters seeking to launder money. There are terror finance risks. The authorities have taken action against Jemaah Islamiyah and its members and have identified and frozen terrorist assets held in Singapore. Structural gaps remain in financial regulations that may hamper efforts to control these crimes. Financial crimes enforcement needs strengthening. To address some of these deficiencies, Singapore is implementing legal and regulatory changes to better align itself with the Financial Action Task Force's (FATF) revised recommendations on anti-money laundering (AML) and counterterrorist financing (CTF).

In September 2007, FATF conducted its Mutual Evaluation of Singapore's AML/CTF regime. The FATF published its findings in February 2008 that Singapore was compliant or largely compliant with most of the FATF Recommendations. The mutual evaluation report noted that, although Singapore's "institutional efforts to improve feedback to financial institutions, enhance supervisory oversight and step up training has resulted in a significant overall strengthening of Singapore's AML/CTF regime, there are remaining concerns about effectiveness of the money laundering offence and the new cross-border declaration system, the requirements applicable to designated nonfinancial businesses and professions (DNFBPs), and the availability of beneficial ownership information in relation to legal persons and arrangements." The Government of Singapore (GOS) intends to address some of the shortcomings by paying more attention to the DFBPs that are susceptible to money laundering risk. The review of the DNFBPs will include the issuing of AML regulations for casino operators and junket promoters.

Singapore's Corruption, Drug Trafficking, and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) has undergone many revisions, with the latest occurring in February 2008. The key amendments added several new categories to its "Schedule of Serious Offenses." The CDSA criminalizes the laundering of proceeds from narcotics transactions and other predicate offenses; including ones committed overseas that would be serious offenses if committed in Singapore. Included among the new offenses are crimes associated with terrorist financing, illicit arms trafficking, counterfeiting and piracy of products, environmental crime, computer crime, insider trading, rigging commodities and securities markets, transnational organized crime, maritime offences, pyramid selling, importation and exportation of radioactive materials/irradiating apparatus, customs offences, falsification or use of false Singapore passports under the Passports Act and terrorist bombings under the Terrorism (Suppression of Bombings) Act 2007. With an eye on Singapore's two new multibillion-dollar casinos slated to be operational in 2009, the list also addresses a number of gambling-related crimes. However, tax and fiscal offenses are still absent from the expanded list.

The Financial Investigation Branch (FIB), located within the Financial Investigation Division of CAD, is the lead money laundering enforcement agency within the Singapore Police Force (SPFC). The work of the FIB is complemented by its sister unit in the SPF, the Proceeds of Crime Unit (PCU). The Central Narcotics Bureau (CNB) is also authorized to investigate ML offences, and has established its own specialist investigative unit (the FIT) to investigate money laundering offences that are related to drug trafficking. Officers of the FIB, PCU and the SPF are empowered to exercise comprehensive

investigative powers, including powers of search, and seizure of evidence in relation to money laundering, terrorist finance, or related predicate offenses. According to the FATF Mutual evaluation, the enforcement regime for investigating money laundering has not been effectively implemented, as is illustrated by the low number of money laundering investigations (approximately 46 as of mid 2007).

Singapore has a sizeable offshore financial sector. As of November 2008, there were 114 commercial banks in operation, including six local and 26 foreign-owned full banks, 40 offshore banks, and 42 wholesale banks. All offshore and wholesale banks are foreign-owned. Singapore does not permit shell banks in either the domestic or offshore sectors. The Monetary Authority of Singapore (MAS), a semi-autonomous entity under the Prime Minister's Office, serves as Singapore's central bank and financial sector regulator, particularly with respect to Singapore's AML/CTF efforts. MAS performs extensive prudential and regulatory checks on all applications for banking licenses, including whether banks are under adequate home country banking supervision. Banks must have clearly identified directors. Unlicensed banking transactions are illegal.

Singapore has increasingly become a center for offshore private banking and asset management. Total assets under management in Singapore grew 32 percent between 2006 and 2007 to Singapore $1.173 trillion (approximately $814 billion), according to MAS.

Beginning in 2000, MAS began issuing a series of regulatory guidelines ("Notices") requiring banks to apply "know your customer" standards, adopt internal policies for staff compliance and cooperate with Singapore enforcement agencies on money laundering cases. Similar guidelines exist for securities dealers and other financial service providers. Banks must obtain documentation such as passports or identity cards from all individual customers to verify names, permanent contact addresses, dates of births and nationalities. Banks must also check the bona fides of company customers. The regulations specifically require that financial institutions obtain evidence of the identity of the beneficial owners of offshore companies or trusts. They also mandate specific record-keeping and reporting requirements, outline examples of suspicious transactions that should prompt reporting, and establish mandatory intra-company point-of-contact and staff training requirements. Similar guidelines and notices exist for finance companies, merchant banks, life insurers, brokers, securities dealers, investment advisors, futures brokers and advisors, trust companies, approved trustees, and money changers and remitters.

Singapore recently revised its AML/CTF regulations for banks and other financial institutions. MAS issued new or revised AML/CTF regulations (in the form of "Notices" and "Guidelines") for banks and other financial institutions, most of which took effect March 1, 2007. Affected institutions include banks, finance companies, merchant banks, moneychangers and remitters, life insurers, capital market intermediaries, and financial advisers. New reporting requirements for originator information on cross-border wire transfers took effect July 1, 2007. The relevant regulations further align certain parts of Singapore's AML/CTF regime more closely with FATF recommendations and specifically address CTF concerns for the first time. Among the recently implemented regulations are new provisions that would proscribe banks from entering into, or continuing, correspondent banking relationships with shell banks; clarify and strengthen procedures for customer due diligence (CDD), including adoption of a risk-based approach; mandate enhanced CDD for foreign politically exposed persons; and additional suspicious transaction reporting requirements. In 2007, Singapore increased the maximum penalty for financial institutions that fail to comply with AML/CTF regulations from Singapore $100,000 (approximately $67,000) to Singapore $1 million ($670,000). The Act also empowers MAS to prosecute financial institution managers in cases where noncompliance is attributable to their consent, connivance or neglect. MAS is considering new regulations for holders of stored value facilities (SVF) to limit the risk of their use for illicit purposes.

In addition to banks that offer trust, nominee, and fiduciary accounts, Singapore has 12 trust companies. All banks and trust companies, whether domestic or offshore, are subject to the same regulation, record-keeping, and reporting requirements, including for money laundering and suspicious transactions. In August 2005, Singapore introduced regulations under the Trust Companies Act (enacted in January 2005 to replace the Singapore Trustees Act) that mandated licensing of trust companies and MAS approval for appointments of managers and directors. MAS issued revised regulations that took effect April 1, 2007 that require approved trustees and trust companies to complete all mandated CDD procedures before they can establish relations with customers. Other financial institutions are allowed to establish relations with customers before completing all CDD-related measures.

Singapore amended its Moneylenders Act in April 2006 to require moneylenders under investigation to provide relevant information or documents. The Act imposes new penalties for giving false or misleading information and for obstructing entry and inspection of suspected premises. Singapore is considering further amendments to strengthen the Act's AML/CTF provisions.

Singapore has issued additional regulations and guidelines governing DNFBPs. The Internal Revenue Authority of Singapore issued AML/CTF guidelines for real estate agents in July 2007. The Law Society of Singapore in August 2007 amended its Legal Profession (Professional Conduct) Rules to strengthen its AML guidelines. Among its provisions, the new rules prohibit attorneys from acting on the behalf of anonymous clients to open or maintain bank accounts or to hold cash or cash instruments.

In April 2005, Singapore lifted its ban on casinos, paving the way for development of two integrated resorts scheduled to open in 2009. Combined total investment in the resorts is estimated to exceed $5 billion. In June 2006, Singapore implemented the Casino Control Act. The Act establishes the Casino Regulatory Authority of Singapore, which will administer the system of controls and procedures for casino operators, including certain cash reporting requirements. Internet gaming sites are illegal in Singapore, under the Common Gaming Houses Act. Payment service providers in Singapore could be prosecuted for an offence when they knowingly provide services that assist an Internet gambling website. Therefore, banks in Singapore have the ability to block credit card payments to Internet casinos with the assistance of credit card companies. Real estate agents, dealers in precious metals and stones, accountants, and trust service providers (other than trust companies) and company service providers do not have AML/CTF obligations with regard to customer due diligence and record keeping.

A person who wishes to engage in for-profit business in Singapore, whether local or foreign, must register under the Companies Act. Every Singapore-incorporated company is required to have at least two directors, one of whom must be resident in Singapore, and one or more company secretaries who must be resident in Singapore. There is no nationality requirement. A company incorporated in Singapore has the same status and powers as a natural person. Bearer shares are not permitted.

Financial institutions must report suspicious transactions and positively identify customers engaging in large currency transactions and are required to maintain adequate records. Since November 1, 2007, Singapore requires in-bound and out-bound travelers to report cash and bearer-negotiable instruments in excess of Singapore $30,000 (approximately $20,000), in accordance with FATF Special Recommendation Nine. Violators are subject to a fine of up to Singapore $50,000 (approximately $33,000) and/or a maximum prison sentence of three years.

The Singapore Police's Suspicious Transaction Reporting Office (STRO) has served as the country's Financial Intelligence Unit (FIU) since January 2000. Procedural regulations and bank secrecy laws limit STRO's ability to provide information relating to financial crimes. In December 2004, STRO concluded a Memorandum of Understanding (MOU) concerning the exchange of financial intelligence with its U.S. counterpart, FinCEN. STRO has also signed MOUs with counterparts in Australia, Belgium, Brazil, Canada, Greece, Hong Kong, Italy, Japan, Mexico and the United Kingdom. To

improve its suspicious transaction reporting, STRO has developed a computerized system to allow electronic online submission of STRs, as well as the dissemination of AML/CTF material. It plans to encourage all financial institutions and relevant professions to participate in this system.

Singapore is an important participant in the regional effort to stop terrorist financing in Southeast Asia. The Terrorism (Suppression of Financing) Act that took effect in January 2003 criminalizes terrorist financing, although the provisions of the Act are actually much broader. In addition to making it a criminal offense to deal with terrorist property (including financial assets), the Act criminalizes the provision or collection of any property (including financial assets) with the intention that the property be used (or having reasonable grounds to believe that the property will be used) to commit any terrorist act or for various terrorist purposes. The Act also provides that any person in Singapore, and every citizen of Singapore outside Singapore, who has information about any transaction or proposed transaction in respect of terrorist property, or who has information that he/she believes might be of material assistance in preventing a terrorist financing offense, must immediately inform the police. The Act gives the authorities the power to freeze and seize terrorist assets.

The International Monetary Fund/World Bank assessment of Singapore's financial sector published in April 2004 concluded that, because Singapore is a party to the UN Convention for the Suppression of the Financing of Terrorism, the country imposes few restrictions on intergovernmental terrorist financing-related mutual legal assistance, even in the absence of a Mutual Legal Assistance Treaty. However, the IMF urged Singapore to improve its mutual legal assistance for other offenses, noting serious limitations on assistance through the provision of bank records, search and seizure of evidence, restraints on the proceeds of crime, and the enforcement of foreign confiscation orders.

Based on regulations issued in 2002, MAS has broad powers to direct financial institutions to comply with international obligations related to terrorist financing. The regulations bar banks and financial institutions from providing resources and services of any kind that will benefit terrorists or terrorist financing. Financial institutions must notify the MAS immediately if they have in their possession, custody or control any property belonging to designated terrorists or any information on transactions involving terrorists' funds. The regulations apply to all branches and offices of any financial institutions incorporated in Singapore or incorporated outside of Singapore, but located in Singapore. The regulations are periodically updated to include names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list.

Singapore's approximately 870,000 foreign guest workers are the main users of alternative remittance systems. As of November 2008, there were 372 moneychangers and 86 remittance agents. All must be licensed and are subject to the Money-Changing and Remittance Businesses Act (MCRBA), which includes requirements for record keeping and the filing of suspicious transaction reports. Firms must submit a financial statement every three months and report the largest amount transmitted on a single day. They must also provide information concerning their business and overseas partners. Unlicensed informal networks, such as hawala, are illegal. In August 2005, Singapore amended the MCRBA to apply certain AML/CTF regulations to remittance licensees and moneychangers engaged in inward remittance transactions. The Act eliminated sole proprietorships and required all remittance agents to incorporate under the Companies Act with a minimum paid-up capital of Singapore $100,000 (approximately $65,000). In July 2007, MAS issued regulations that require licensees to establish the identity of all customers. MAS must approve any non face-to-face transactions.

Singapore has five free trade zones (FTZs), four for seaborne cargo and one for airfreight, regulated under the Free Trade Zone Act. The FTZs may be used for storage, repackaging of import and export cargo, assembly and other manufacturing activities approved by the Director General of Customs in conjunction with the Ministry of Finance.

Charities in Singapore are subject to extensive government regulation, including close oversight and reporting requirements, and restrictions that limit the amount of funding that can be transferred out of

Singapore. Singapore had approximately 1900 registered charities as at end 2007. All charities must register with the Commissioner of Charities that reports to the Minister for Community Development, Youth and Sports. Charities must submit governing documents outlining their objectives and particulars of all trustees. The Commissioner of Charities has the power to investigate charities, search and seize records, restrict the transactions into which the charity can enter, suspend staff or trustees, and/or establish a scheme for the administration of the charity. Charities must keep detailed accounting records and retain them for at least seven years.

Changes to the Charities (Registration of Charities) Regulations that came into effect in May 2007 authorize the Commissioner to deregister charities deemed to be engaged in activities that run counter to the public interest. Singapore has also implemented tighter rules under the Charities Act that govern public fund-raising by charities, effective May 1, 2007. Charities authorized to receive tax-deductible donations are required to disclose the amount of funds raised in excess of Singapore $1 million (approximately $670,000), expenses incurred, and planned use of funds. Under the Charities (Fund-raising Appeals for Foreign Charitable Purposes) Regulations (1994), any charity or person that wishes to conduct or participate in any fund-raising for any foreign charitable purpose must apply for a permit. The applicant must demonstrate that at least 80 percent of the funds raised will be used in Singapore, although the Commissioner of Charities has discretion to allow for a lower percentage. Permit holders are subject to additional record-keeping and reporting requirements, including details on every item of expenditure, amounts transferred to persons outside Singapore, and names of recipients. The government issued 27 permits in 2007 and 66 permits as of November 2008 related to fundraising for foreign charitable purposes. There are no restrictions or direct reporting requirements on foreign donations to charities in Singapore.

To regulate law enforcement cooperation and facilitate information exchange, Singapore enacted the Mutual Assistance in Criminal Matters Act (MACMA) in March 2000. Parliament amended the MACMA in February 2006 to allow the government to respond to requests for assistance even in the absence of a bilateral treaty, MOU or other agreement with Singapore. The MACMA provides for international cooperation on any of the 292 predicate "serious offenses" listed under the CDSA. In September 2008, the government introduced an amendment to the Terrorism (Suppression of Financing) Act to allow the government to respond to requests for extradition even in the absence of an extradition treaty for all terrorism financing offences.

In November 2000, Singapore and the United States signed the Agreement Concerning the Investigation of Drug Trafficking Offenses and Seizure and Forfeiture of Proceeds and Instrumentalities of Drug Trafficking (Drug Designation Agreement or DDA). This was the first agreement concluded pursuant to the MACMA. The DDA, which came into force in early 2001, facilitates the exchange of banking and corporate information on drug money laundering suspects and targets, including access to bank records. It also entails reciprocal honoring of seizure/forfeiture warrants. This agreement applies only to narcotics cases, and does not cover non-narcotics related money laundering, terrorist financing, or financial fraud.

In May 2003, Singapore issued a regulation pursuant to the MACMA and the Terrorism Act that enables the government to provide legal assistance to the United States and the United Kingdom in matters related to terrorist financing offenses. Singapore concluded mutual legal assistance agreements with Hong Kong in 2003, India in 2005, and Laos in 2007. Singapore is a party to the ASEAN Treaty on Mutual Legal Assistance in Criminal Matters along with Malaysia, Vietnam, Brunei, Cambodia, Indonesia, Laos, the Philippines, Thailand, and Burma. The treaty will come into effect after ratification by the respective governments. Singapore, Malaysia, Laos, Vietnam and Brunei have ratified thus far.

In addition to the UN Convention for the Suppression of the Financing of Terrorism, Singapore is also a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized

Crime. It has signed, but not ratified, the UN Convention against Corruption. In addition to FATF, Singapore is a member of the Asia/Pacific Group (APG) on Money Laundering, the Egmont Group, and the Offshore Group of Banking Supervisors.

Singapore should continue close monitoring of its domestic and offshore financial sectors. The government should add tax and fiscal offenses to its schedule of serious offenses. The government should also act quickly to rectify the weaknesses identified in the FATF Mutual Evaluation Report to strengthen its AML/CTF enforcement abilities. The conclusion of broad mutual legal assistance agreements is also important to further Singapore's ability to work internationally to counter money laundering and terrorist financing. Singapore should lift its rigid bank secrecy restrictions to enhance its law enforcement cooperation in areas such as information sharing and to conform to international standards and best practices. Singapore should also strictly enforce border controls and give greater attention to trade-based money laundering. Singapore should become a party to the UN Convention against Corruption.

Slovak Republic

Slovakia's geographic, economic, and legal environment with respect to money laundering are not atypical of a changing central European economy. Its geographical location makes it a transit country for trafficking in drugs, people, and a variety of commodities. The statistics on money laundering cases investigated by Slovak law enforcement authorities since 2004 indicate the most frequent predicate offense for money laundering is motor vehicle theft. According to data from reporting entities, in 2007, the most commonly reported forms of suspicious activity were Internet fraud involving funds originating in the United States; phishing involving funds originating in Germany, Switzerland, the United Kingdom and the United States; use of tax havens and offshore companies for transfers of funds; and trafficking in nonferrous metals and investment gold.

The Penal Code criminalizes money laundering through Section 233 (legalization of income from criminal activity), which depending on the circumstances of the crime, calls for sentences of two to 20 years' imprisonment. The Penal Code also criminalizes other criminal offenses such as creating, contriving to create, or supporting a terrorist group (Section 297) as well as the offense of terrorism (Section 419). One area lacking in the Slovak Penal Code or in an autonomous law is the criminal liability of legal persons.

The Penal Code (Act No. 300/2005 Coll., as amended) and the Code of Criminal Procedure (Act No. 301/20005 Coll., as amended), effective since January 2006, introduce several changes to the criminal legislation. These changes result in stricter sentences for most criminal offenses and seek to make criminal procedure more efficient in order to ensure a more effective protection of the rights and interests of legal and natural persons. Slovak legislation does not specifically list the predicate offenses for money laundering. The criminal offense of money laundering can be prosecuted if criminal prosecution is already pending for a predicate criminal offense.

The Code of Criminal Procedure provides law enforcement and judicial authorities effective instruments that can be used to combat money laundering, such as seizure of cash (Section 95) or of registered securities (Section 96). The Code also makes it possible to secure the claims of injured parties (Section 50) and to hand down sentences involving the property of sentenced persons, such as forfeiture of property (Section 428).

Slovakia's anti-money laundering (AML) legislation has evolved substantially since 1994 when it adopted its first AML law, Act No. 249/1994 Coll. Since 1994, Act No. 249/1994 Coll. has undergone two revisions, first in 2000, and most recently in 2008. The 2008 changes became effective in September and were codified as Act No. 297/2008 Coll., "On the Protection Against Legalization of Income from Criminal Activity and Protection Against the Financing of Terrorism." The 2008 law

defines basic notions such as "legalization" (Section 2), "terrorist financing" (Section 3), and "unusual transaction" (Section 4). It also includes more precise definitions of "reporting entities" (Section 5) and "politically exposed person" (Section 6); and contains separate provisions on lawyers and notaries (Section 22); and auditors, accountants and tax advisors (Section 23). With regard to safe harbour provisions, the 2008 law includes enhanced protection from threats by third parties or by persons involved in unusual transactions for employees who report unusual transactions. The law also introduces the possibility of exchanging information on unusual transactions between reporting entities and obligates reporting entities to prepare anti-money laundering/counterterrorist financing (AML/CTF) compliance programs, setting out mandatory components of such programs. The 2008 law also enumerates for reporting entities certain unusual transactions relating to money laundering and terrorist financing.

Act No. 297/2008 Coll. sets out the detailed conditions for performing customer due diligence (Section 10), simplified due diligence (Section 11) and enhanced due diligence (Section 12). Reporting entities have a duty to perform customer due diligence that includes, in particular, client identification and verification as well as identification of the beneficial owner in the case of legal persons or property associations. For corporations, it includes the identification of ownership and management structure if the customer enters into a business relationship, envisages or performs an unusual transaction irrespective of its value, or performs an occasional transaction with a value of at least EUR 15,000 (approximately $20,250) outside of a business relationship, regardless of whether the transaction is carried out as a single transaction or as several consecutive transactions which are or could be linked. The law uses a risk-based approach to specify customer due diligence obligations, including exemptions from due diligence obligations, and enhanced due diligence for "higher-risk customers." Reporting entities are entitled to ask customers to provide information and documents necessary for due diligence purposes. The 2008 law also provides the basis for exemption of financial activities conducted on an occasional or very limited basis.

Reporting entities are obliged to give special attention to business relationships and transactions with persons from or in countries that do not apply, or insufficiently apply, the Financial Action Task Force (FATF) Recommendations, and to perform enhanced customer diligence in such cases. Under Act No. 297/2008 Coll., reporting entities must meet this obligation in the case of cross-border correspondent banking relationships with credit institutions from non-European Union (EU) member states by obtaining information from publicly accessible sources about the respondent credit institution.

As a result of 2001 amendments to the Slovak Civil Code, the Government of Slovakia (GOS) ordered all banks to stop offering anonymous accounts. All existing owners of anonymous accounts were required to disclose their identity to the bank and close the anonymous account by December 31, 2003. Owners of accounts that were still open could withdraw money for a three-year non-interest bearing grace period. The GOS confiscated all account balances remaining after January 1, 2007, and deposited them in a fund administered by the Ministry of Finance, where they will be available for collection by the account holder until January 1, 2012. As of January 1, 2007, bearer passbook accounts ceased to exist.

The Slovak Republic adopted Regulation 1781/2006 of the European Parliament and of the Council of November 15, 2006, to require that wire transfer originator data accompany transfers of funds.

The Slovak Financial Intelligence Unit (SFIU) was established in 1996 and is currently within the structure of the Police Corps Presidium's Bureau for Combating Organized Crime (BCOC). The BCOC deals with all forms of organized crime, including drugs, money laundering, and human trafficking. The BCOC has four regional sections (Bratislava, West, Center, and East). The SFIU is the fifth section of the BCOC, with nation-wide authority. The SFIU has four departments: the Unusual Transactions Department, the Obliged Entities Supervision Department, the International Cooperation Department, and the Property Checks Department. The SFIU, as the organization responsible for

combating money laundering and terrorist financing within the meaning of Act No. 297/2008 Coll., receives and evaluates suspicious transaction reports (STRs), gathers additional information, and refers cases of suspected money laundering to regional financial police departments, other law enforcement authorities or tax administrators, as appropriate.

The Obliged Entities Supervision Department of the SFIU is the only supervisory body vested with the authority to assess the AML/CTF compliance of covered entities, including designated nonfinancial businesses and professions (DNFBPs). In case of noncompliance, the SFIU imposes fines or initiates the withdrawal of the authorization to perform entrepreneurial or other gainful activity. In an effort to promote effective application of Act No. 297/2008 Coll., the SFIU is providing training stressing the importance of strengthening internal compliance programs to reporting entities through associations and professional organizations. According to the SFIU, there are approximately 100,000 reporting entities in Slovakia. In 2007, the Department carried out 45 checks on reporting entities and imposed total fines of SKK 1,080,000 (approximately $48,000). In the first half of 2008, the Department conducted 28 checks of reporting entities and imposed fines totaling SKK 325,000 (approximately $14,400). Only banks and insurance agencies are submitting reports on a regular basis, with the securities sectors submitting reports irregularly. In 2006, the SFIU received one report from an exchange office. Sporadic compliance by DNFBPs was observed in 2007, with three reports received from tax advisors, two from lawyers, and one from a real estate agency. As of November 24, 2008, the SFIU received two reports from executors, five from notaries, and one from an auditor. No reports have yet been received from a casino.

In 2006, the SFIU received 1,571 STRs totaling SKK 22,120,760 (approximately $983,000). Based on these reports, 26 cases were referred to law enforcement authorities, 108 to regional financial police departments, 438 to tax administrators, and 84 to financial intelligence units (FIUs) abroad.

In 2007, the SFIU received 1,943 STRs totaling SKK 18,913,584 (approximately $840,000). Based on these reports, 12 cases were referred to law enforcement authorities, 194 to regional financial police departments or other specialized departments, 582 to tax administrators, and 125 to foreign FIUs.

As of October 29, 2008, the SFIU received 1,814 STRs totaling SKK 21,535,397 (approximately $957,000). Based on these reports, nine cases were referred to law enforcement authorities, 248 to regional financial police departments or other specialized departments, 399 to tax administrators, and 161 to foreign FIUs.

According to statistical overviews published by the General Prosecution Office of the Slovak Republic, six persons were subject to criminal proceedings in Slovakia in 2006 for the offense of money laundering pursuant to Section 233; only one of these individuals has been convicted. In 2007, criminal proceedings were conducted against six persons, one of whom was convicted. Statistics for 2008 are not yet available. Measures adopted at the SFIU level through the President of the Police Force seek to increase the transparency and degree of detail of statistical data gathered by the Police Force, incorporating into the criminal file data obtained as feedback from prosecution authorities and courts. It is anticipated these measures will effectively implement Act No. 297/2008 Coll., which obliges the Police Force to keep aggregate statistics on the number of persons sentenced for money laundering and on the value of seized, forfeited or confiscated assets.

Reporting entities have a duty to halt the execution of unusual transactions for a maximum of 48 hours either on the basis of their own finding or upon written request from the SFIU. If the investigation confirms the suspicion of a criminal offense, the SFIU refers the matter to the relevant law enforcement authority; in such cases, the reporting entity has a duty to halt the execution of the transaction for another 24 hours. Reporting of an unusual transaction does not exempt the reporting entity from its obligation to report the suspected criminal offense to law enforcement authorities. Should any damage be caused as a result of reporting or halting an unusual transaction, damage compensation is paid by the state.

Slovak law mandates forfeiture of the proceeds of crime. It does not, however, allow for forfeiture from third-party beneficiaries. The Office of the Public Prosecutor may order the seizure of accounts during the pre-trial proceedings stage, and can order the use of information technology for enhanced investigations under Articles 79c, 88 and 88e of the Criminal Procedure Code. In 2006, a new Confiscation Law became effective, strengthening the government's ability to seize assets gained through criminal activity. Effective January 1, 2006, Act No. 650/2005 Coll. gives Slovakian authorities the power to execute a seizure order on property within the territory of the Slovak Republic even if the order was issued by a judicial authority of another member state of the EU.

The Law on Proving the Origin of Property came into force on September 1, 2005. According to this law, an undocumented increase in property exceeding an amount 200 times the minimum monthly wage must be scrutinized. The police must investigate allegations of illegally acquired property and report their findings to the Office of the Public Prosecutor, which may then order the property confiscated. The law was challenged in Parliament on the grounds that its retroactivity and shifting of the burden of proof to the suspect are in conflict with the Constitution of the Slovak Republic. The Constitutional Court suspended application of the law on October 6, 2005. On September 3, 2008, the Constitutional Court issued a finding which determined the law is not in conformity with the Constitution of the Slovak Republic. The National Council of the Slovak Republic has a six-month time limit to repeal the law; alternatively, it may adopt a new law replacing the existing one. The existing law will automatically become null and void if neither of these measures is taken.

The Penal Code does not yet define terrorist financing, per se, as an autonomous criminal offense. Section 3 of Act No. 297/2008 Coll. defines the financing of terrorism as the supply or collection of funds with the intent to use them or with the knowledge of the intent to use them in the commission of the criminal offense of creating, contriving to create or supporting a terrorist group, or the criminal offense of terrorism, or other criminal offenses referred to in Section 3(1)(b) of the law.

All competent authorities in the Slovak Republic have full authority to freeze or confiscate terrorist assets consistent with UNSCR 1373. The GOS has agreed to immediately freeze all accounts owned by entities included on the UNSCR 1267 Sanctions Committee Consolidated List of terrorist entities, the EU's consolidated lists, and those provided by the United States under Executive Order 13224. The GOS posts the lists online but does not distribute them. Reporting entities are responsible for checking the website and reporting any matches they find. In the event a reporting entity were to identify a terrorism-related account, the SFIU could suspend any related financial transaction for up to 48 hours, and then gather evidence to freeze the account and seize assets.

The reporting obligation regarding terrorist financing is laid down in Act No. 297/2008 Coll. Although the SFIU has not received any STRs with the specific suspicion of terrorist financing, the SFIU assessed the reports received in the period of 2006–2008 for possible links to terrorist organizations or suspicions of terrorist financing, and referred the relevant information to the Department for Combating Terrorism within the BCOC. The SFIU searched mainly for transfers of funds involving persons or companies originating or having a seat in areas with a high risk of links to terrorist organizations. In 2006, the SFIU referred information on 14 cases; in 2007, 27 cases; and through August 2008, ten cases.

The SFIU is a member of the Egmont Group. The SFIU has signed nine memoranda of understanding (with Slovenia, Canada, Belgium, Czech Republic, Poland, Monaco, Australia, Ukraine and Albania), two cooperation protocols (with Czech Republic and Ukraine) and two cooperation agreements (with Russia and Romania). Slovak law does not, however, require that the SFIU sign a memorandum of understanding to be able to fully cooperate with FIUs in other countries.

Slovakia is a member of the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), a FATF-style regional body. The third round mutual evaluation report by MONEYVAL was adopted in September 2006, and

Slovakia is scheduled to undergo its fourth round mutual evaluation in 2009. Slovakia is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the UN Convention for the Suppression of the Financing of Terrorism.

While the Government of Slovakia has made progress over the past year, several areas of its AML/CTF regime still require further work. The competent authorities should ensure the wording of Section 252 of the Penal Code clearly defines the property and proceeds of crime. Slovakia should also provide capacity enhancing materials to DNFBPs and improve supervision of these entities to ensure they meet their obligations under the law. Slovakia should implement formal AML/CTF supervision of currency exchange houses. Slovak authorities should encourage and enable police to pursue money laundering and financial crime even when it does not involve organized crime activities. The GOS should provide adequate resources to ensure the FIU, law enforcement, and prosecutorial agencies receive adequate funding and training, as well as maintain adequate staff, to effectively perform their various responsibilities; the FIU in particular needs staffing commensurate with its responsibilities. The GOS should work to enhance cooperation and coordination among these agencies and other competent authorities. Authorities should adopt criminal, civil, or administrative sanctions for money laundering in relation to legal persons. The GOS should consider amending its confiscation and forfeiture regime to provide for asset forfeiture from third-party beneficial owners. The Slovak government should proactively provide the lists of individuals linked with terrorism by the UN, the EU, and the United States to reporting entities, and thus, introduce stricter procedures for combating terrorist financing. The GOS also should codify reporting obligations for nonprofit organizations and charities. Competent authorities should amend the Penal Code to criminalize terrorist financing.

South Africa

South Africa's position as the major financial center in the region, its relatively sophisticated banking and financial sector, and its large, cash-based market, make it a vulnerable target for transnational and domestic crime syndicates. The largest quantity of illicit proceeds laundered in the country are proceeds from the narcotics trade. Proceeds from fraud, theft, corruption, currency speculation, illicit dealings, theft of precious metals and diamonds, small arms, human trafficking, stolen cars, and smuggling are also laundered. Most criminal organizations are also involved in legitimate business operations. There is a significant black market for smuggled and stolen goods. In addition to South African criminal organizations, observers note the operations of Nigerian, Pakistani, Andean and Indian drug traffickers, Chinese triads, Taiwanese groups, Lebanese trading syndicates, and the Russian mafia. The fact that a high number of international crime groups operate in South Africa and a lack of money laundering prosecutions reported indicate that South Africa remains vulnerable to all-source money laundering.

South Africa is not an offshore financial center, nor does it have free trade zones. It does, however, operate Industrial Development Zones (IDZs). Imports and exports that are involved in manufacturing or processing in the zones are duty-free, provided that the finished product is exported. South Africa maintains IDZs in Port Elizabeth, East London, Richards Bay, and Johannesburg International Airport. The South African Revenue Service (SARS) monitors the customs control of these zones.

SARS requires all visitors carrying cash to declare the amount upon arrival in South Africa. All South African citizens and residents leaving the country with cash must declare amounts in excess of 175,000 rand ($17,500) for individuals, or 250,000 rand ($25,000) for families. Although South Africa has not explicitly criminalized bulk cash smuggling, failing to declare currency carries a penalty. Smuggling and reportedly lax border enforcement pose major vulnerabilities for South Africa.

The Proceeds of Crime Act (No. 76 of 1996) originally criminalized money laundering for all serious crimes. South Africa replaced this act with the Prevention of Organized Crime Act (No. 121 of 1998),

which confirms the criminal character of money laundering, mandates the reporting of suspicious transactions, and contains "safe harbor" provisions. Violation of this act carries a fine of up to 100 million rand ($10 million) or imprisonment for up to 30 years.

The Financial Intelligence Centre Act (FICA) requires a wide range of financial institutions and businesses to identify customers, maintain records of transactions for at least five years, appoint compliance officers to train employees to comply with the law, and report transactions of a suspicious or unusual nature. Both the Prevention of Organized Crime Act and the FICA contain criminal and civil forfeiture provisions. Regulators include the South African Reserve Bank and the Financial Services Board. Regulated businesses include banks, life insurance companies, foreign exchange dealers, casinos, and real estate agents. Additional amendments to the FICA became law on August 27, 2008. The amendments strengthen the ability of regulators to supervise private sector compliance with FICA mandates and obligations. They also enhance the financial intelligence unit's (FIU) power to oversee overall FICA compliance and coordinate with regulators. The amendments strengthen the power of the FIU and regulators to conduct inspections, request information, and impose financial administrative sanctions. In addition to the FIU, South Africa has a Money Laundering Advisory Council (MLAC) to advise the Minister of Finance on policies and measures to combat money laundering.

Conforming to the money laundering regime has been expensive for banks, which have re-registered customers, given AML training to employees, expanded their internal compliance offices, and taken other steps to comply with the law. Many banks state that the reporting requirements hamper their efforts to attract new customers. For example, if customers have never traveled outside the country, they may not have supporting documentation (driver's license or passport) to properly satisfy the due diligence requirements. Retroactive due diligence requirements mean those account holders who do not present identifying documents in person risk having their accounts frozen. After the September 2006 implementation of the requirements, financial institutions blocked transactions with accounts owned by still-unidentified persons. In part due to the stricter banking requirements, but also because of the cash-driven nature of the South African economy, South Africans, particularly the Muslim and Indian communities, often use alternative remittance systems that bypass the formal financial sector. Hawala networks in South Africa have direct ties to both South Asia and the Middle East. Currently, South Africa does not require alternative remittance providers or participants to report cash transactions within the country.

Regulations require suspicious transaction reports to be sent to the South African FIU, called the Financial Intelligence Centre (FIC). The FIC, in operation since 2003, gathers and analyzes financial intelligence for law enforcement authorities to use in pursuit of money laundering and other financial crimes, and acts as a centralized repository of information and statistics on money laundering. It also coordinates policy and anti-money laundering efforts. If the FIC has reasonable grounds to suspect that a transaction involves the proceeds of criminal activities, it forwards the transactional information to the investigative and prosecutorial authorities. When there is a suspicion of terrorist financing, the FIC will forward the relevant information to the National Intelligence Agency. There are no bank secrecy laws in effect that prevent the disclosure of ownership information to bank supervisors and law enforcement authorities.

From March 2007 through March 2008, the FIC received 24,580 suspicious transaction reports (STRs), an increase of fifteen percent from the previous year's 21,466 STRs. Ninety-one percent of the reports came from financial institutions, with the remainder generated by casinos, coin dealers, accountants, attorneys, and other reporting entities. The FIC referred 999 STRs, with transactions valued at more than 2.03 billion rand ($200 million), to law enforcement and/or intelligence agencies for further investigation. The FIC and banking officials report that the quality of the STRs is steadily improving, as bank personnel receive AML training and as institutions install and refine AML software and other detection systems. Between 2007 and 2008, the FIC joined regulators in conducting

212 on-site anti-money laundering/counterterrorist financing (AML/CTF) compliance reviews of casinos, foreign exchange dealers, insurance companies, and other institutions. The FIC also conducted 27 independent compliance reviews.

Information is not available on the number of STRs resulting in criminal investigations. However, the number of money laundering and terrorist finance investigations, prosecutions, and convictions is reportedly very low. The corruption case filed against ANC President Jacob Zuma in December 2006 included money-laundering charges, but a High Court dismissed the indictment in September 2008 because of procedural flaws unrelated to the money-laundering charges. The case is now under appeal. In February 2008, Graham Maddock, the financial director of scandal-plagued Fidentia Group, pled guilty to, inter alia, money-laundering charges and violations of the FICA, marking the first successful prosecution of a FICA violation. While progress has been made regarding criminal enforcement of AML/CTF violations, the low number of cases prosecuted suggests possible problems in reporting, analysis, and investigations. Many investigators and prosecutors appear to focus on predicate offenses, which indicates they may lack familiarity with money laundering offenses or see no reason to add money laundering charges to cases.

In 2005, the Protection of Constitutional Democracy Against Terrorist and Related Activities Act came into effect. The Act criminalizes terrorist activity and terrorist financing and gave the government investigative and asset seizure powers in cases of suspected terrorist activity. The Act requires financial institutions to report suspected terrorist activity to the FIC. The Act also applies to charitable and nonprofit organizations operating in South Africa. The FIC distributes the list of individuals and entities included on the United Nations (UN) 1267 Sanctions Committee's consolidated list.

South Africa cooperates with the United States in exchanging information related to money laundering and terrorist financing. The two nations have a mutual legal assistance treaty and a bilateral extradition treaty (litigation regarding the status of the extradition treaty is now before the South African Constitutional Court). In June 2003, South Africa became the first African nation to be admitted into the Financial Action Task Force (FATF), and held the FATF Presidency for the period June 2005-June 2006. At the end of 2008, South Africa underwent a mutual evaluation which is scheduled for discussion and adoption by that body in 2009. South Africa is also a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. The FIC is a member of the Egmont Group. South Africa is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption.

The South African Government should fully implement FATF Special Recommendation IX, including the establishment of controls for cross-border currency movements. South Africa should increase steps to bolster border enforcement and examine trade-based money laundering. It should also regulate and investigate the country's alternative remittance systems, and further examine their use and vulnerability to exploitation by money launderers and terrorist financiers. Authorities should ensure that FIC analysts and law enforcement look beyond STR reporting to initiate money laundering investigations. Law enforcement and customs officials should follow the money and value trails during the course of their investigations to determine if money laundering has occurred. South Africa should also continue to enforce AML regulations within the casino industry. It should fully implement the new law against terrorist activity and terrorist financing. South Africa should publish the annual number of money laundering and terrorist financing investigations, prosecutions, and convictions.

Spain

Spain is a major European center of money laundering activities as well as a major gateway for illicit narcotics. Drug proceeds from other regions enter Spain as well, particularly proceeds from Afghan

hashish entering from Morocco, cocaine entering from Latin America, and heroin entering from Turkey. There are no known currency transactions of significance involving large amounts of U.S. currency and/or direct narcotics proceeds from U.S. sales.

Tax evasion in internal markets and the smuggling of goods along the coastline also continue to be sources of illicit funds in Spain. The smuggling of electronics and tobacco from Gibraltar remains an ongoing problem. Passengers traveling from Spain to Latin America reportedly smuggle sizeable sums of bulk cash. Additional money laundering activities found in Spain include Colombian companies purchasing goods in Asia and selling them legally at stores run by drug cartels in Europe. Credit card balances are paid in Spanish banks for charges made in Latin America, and money deposited in Spanish banks is withdrawn in Colombia through ATM networks.

An unknown percentage of drug-trafficking proceeds are invested in Spanish real estate, particularly in the once-booming coastal areas in the south and east of the country. Up to thirty percent of the 500 euro notes in use in Europe are reported to be in circulation in Spain, directly linked to the purchase of real estate to launder money. In the past year however, Spain's tax authority has cracked down on fraudulent activity involving these large bank notes and as a result the number of 500 euro notes has decreased to October 2006 levels of 110 million euros (approximately $148,500,000).

Throughout 2008, Spanish authorities conducted numerous anti-money laundering (AML) and counterterrorist financing (CTF) operations that resulted in arrests. On June 10, Spanish authorities arrested eight Algerian nationals reportedly linked to terrorist financing activities of al-Qaida in the Islamic Maghreb (AQIM). These arrests were made under "Operation Submarine", an operation which led to other arrests throughout the year of Algerian nationals linked to the same cell. On June 17, Spanish authorities dismantled an international criminal organization accused of money laundering and cocaine smuggling operations, arresting 21 individuals including nationals of Spain, Colombia, Peru, and Romania. On September 19, Spanish national police arrested nine people in the northern Basque region suspected of participating in a money laundering ring, sending to Latin America more than 32 million euros (approximately $43,200,000) since 2006.

The Financial Action Task Force (FATF) 2006 Mutual Evaluation Report (MER) noted shortcomings in the areas of customer due diligence, beneficial ownership of legal persons, and the use of bearer shares which have yet to be completely corrected.

Spanish authorities recognize the presence of alternative remittance systems. Informal nonbank outlets such as "locutorios" (communication centers that often offer wire transfer services) are used to move money in and out of Spain by making small international transfers for members of the immigrant community. Spanish regulators also note the presence of hawala networks in the Islamic community.

Spain is not considered to be an offshore financial center and does not operate any free trade zones. Spanish law states that an entity can perform banking activity if its registered office, administration, and management reside within Spanish territory. Spanish law does not prohibit financial institutions from entering into banking relationships with shell banks, but there are no shell banks in Spain. Financial institutions have no requirement to determine whether a correspondent financial institution in a foreign country allows accounts used by shell banks. Offshore casinos and Internet gaming sites are forbidden, but online casinos often run from servers located outside of Spanish territory. In this instance, regulation can only occur through mutual judicial assistance or international agreements.

Although there was little AML/CTF legislative activity in 2008, the Government of Spain (GOS) has passed and enacted legislation designed to help eliminate and prosecute financial crimes. Money laundering is criminalized by Article 301 of the Penal Code, added in 1988 when laundering the proceeds from narcotics-trafficking was made a criminal offense. Individuals in fiduciary institutions can be held liable if their institutions have been used to commit financial crimes; a 1991 amendment made such persons culpable for both fraudulent acts and negligence connected with money laundering.

The law was expanded in 1995 to cover all serious crimes that require a prison sentence greater than three years. Amendments to the code, which took effect in 2004, make all forms of money laundering financial crimes. Any property, of any value, can form the basis for a money laundering offense, and a conviction or a prosecution for a predicate offense is not necessary to prosecute or obtain a conviction for money laundering. Spanish authorities can also prosecute money laundering based on a predicate offense in another country, if the predicate offense would be a crime in Spain.

Law 19/2003 obliges financial institutions to make monthly reports on large transactions. Banks are required to report all international transfers greater than 50,000 euros (approximately $67,500). The law also requires the declaration and reporting of internal transfers of funds greater than 100,000 euros (approximately $135,000). Individuals traveling internationally are required to report the importation or exportation of currency greater than 10,000 euros (approximately $13,500). Foreign exchange and money remittance entities must report transactions above 5,000 euros (approximately $6,750). Authorities also require the reporting of transactions exceeding 50,000 euros (approximately $67,500) from or with persons in countries or territories considered to be tax havens. Law 19/2003 allows the seizure of up to 100 percent of the currency if illegal activity under financial crimes ordinances can be proven. Spanish authorities claim they have seen a drop in cash couriers since the law's enactment in July 2003. When the money has not been declared and cannot be connected to criminal activity, authorities may seize it until the origin of the funds is proven.

Money laundering controls apply to most entities active in the financial system, including banks, mutual savings associations, credit companies, insurance companies, financial advisers, brokerage and securities firms, pension fund managers, collective investment schemes, postal services, currency exchange outlets, and individuals and unofficial financial institutions exchanging or transmitting money. Most categories of designated nonfinancial businesses and professions (DNFBPs) are subject to the same core obligations as the financial sector. The list of DNFBPs includes realty agents; dealers in precious metals, stones, antiques and art; legal advisors and lawyers; accountants; auditors; notaries; and casinos.

The financial sector is required to identify customers, keep records of transactions, and report suspicious transactions. Spanish financial institutions are required by law to maintain fiscal information for five years and mercantile records for six years. Financial institutions are required to monitor transactions and report anything they deem unusual or potentially problematic. Reporting entities are required to examine and commit to writing the results of an examination of any transaction, irrespective of amount, which by its nature may be linked to laundering of proceeds. Law 12/2003 reaffirms the obligation of reporting suspicious activities. Reporting entities are required to report each suspicious transaction to the financial intelligence unit (FIU). Financial institutions also have an obligation to undertake systematic reporting of unusual transactions and those exceeding the currency threshold, including physical movements of cash, travelers' checks, and other bearer instruments/checks drawn on credit institutions above 50,000 euros (approximately $67,500).

Article 4 of Law 19/1993 and Article 15 of Royal Decree (RD) 925/1995 contain safe harbor provisions. Financial institutions and their staffs are legally protected from any breach of restrictions on disclosure of information when reporting suspicious transactions. Reporting units must also take appropriate steps to conceal the identity of employees or managers making suspicious transaction reports (STRs).

Anonymous accounts and accounts in fictitious names are precluded by Spanish legislation. Bearer shares are permitted in Spain, although they are not as prevalent as they have been in the past. Spanish authorities have taken steps to neutralize them since 1998, ensuring that mere possession cannot serve as proof of ownership. However, they still exist, and the FATF MER cited the requirements to determine the beneficial owner as "inadequate."

Law 19/1993 and RD 925/1995 establish the Executive Service of the Commission for the Prevention of Money Laundering (SEPBLAC) as Spain's FIU. Its primary mission is to receive, analyze, and disseminate suspicious and unusual transaction reports from financial institutions and DNFBPs. SEPBLAC has primary responsibility for any investigation in money laundering cases. SEPBLAC also has supervisory and inspection functions and is directly responsible for the supervision of a large number of regulated institutions; for example, it directly supervises the AML procedures of banks and financial institutions. SEPBLAC thus has memoranda of understanding with the Bank of Spain, the National Securities Market Commission, and the Director General of Insurance and Pension Funds, to coordinate with the regulators that supervise their respective sectors.

SEPBLAC supports the work of the Commission for the Prevention of Money Laundering (CPBC or "Commission") which coordinates policy in the fight against money laundering in Spain. The Commission is an interdepartmental body chaired by the Second Vice President and Minister for Economic Affairs, with participation from the heads of agencies involved in the prevention of money laundering. These agencies include the National Drug Plan Office, the Ministry of Economy, Federal Prosecutors (Fiscalia), Customs, Spanish National Police, Civil Guard, CNMV (equivalent to the U.S. Securities and Exchange Commission), Treasury, Bank of Spain, and the Director General of Insurance and Pension Funds. Within the Ministry of Economy and Finance, the Sub Directorate General of Inspection and Control of Movements (Sub Directorate General) serves as the Commission's Secretariat as well as Spain's FATF representative office. The Sub Directorate General is responsible for preparing draft rules and regulations and implementing financial sanctions in accordance with Law 19/1993.

The Bank of Spain is responsible for appointing SEPBLAC's director, raising concerns regarding the FIU's independence. Additionally, the FIU's supervisory capabilities continue to be hampered by its limited resources. In SEPBLAC's annual report, the organization acknowledged these weaknesses and expressed a desire to work to address these issues.

SEPBLAC has access to the records and databases of other government entities and financial institutions. It also has formal mechanisms in place to share information domestically and with other FIUs. SEPBLAC has been a member of the Egmont Group since 1995. In 2007, SEPBLAC received 2,783 STRs, up from 2,251 in 2006. SEPBLAC received 590 requests for information from other FIUs in 2007 and made 193 requests to Egmont members.

Any member of the Commission may request an investigation. However, at certain stages of the investigative process, obtaining account files can be time-consuming. The National Police and Anticorruption Police informed the FATF evaluation team that they receive too many reports, and the reports they do receive are not adequate to serve as the basis for an investigation.

The Sub Directorate General has the responsibility to carry out penalties following investigation and a guilty verdict by a court. Sanctions can include closure, fines, account freezes, or seizures of assets. Law 19/2003 allows seizures of assets of third parties in criminal transactions and a seizure of real estate in an amount equivalent to the illegal profit.

Individuals and companies must declare the amount, origin, and destination of incoming and outgoing funds. Cash smuggling reports are shared between host government agencies. Provisional measures and confiscation provisions apply to persons smuggling cash or monetary instruments that are related to money laundering or terrorist financing. Gold, precious metals, and precious stones are considered to be merchandise and are subject to customs legislation. Failing to file a declaration for such goods may constitute a case of smuggling and would fall under the responsibility of the customs authorities.

All legal charities are placed on a register maintained by the Ministry of Justice. Responsibility for policing registered charities lies with the Ministry of Public Administration. If a charity fails to comply with the requirements, sanctions or other criminal charges may be levied.

The Penal Code provides for two types of confiscation: generic (Article 127) and specific, for drug-trafficking offenses (Article 374). Article 127 of the Penal Code allows for broad confiscation authority by applying it to all crimes or summary offenses under the Code. The effects and instruments used to commit the offense, and the profits derived from the offense can all be confiscated. Article 127 also provides for the confiscation of property intended for use in the commission of any crime or offense. It also applies to property that is derived directly or indirectly from proceeds of crime, regardless of whether the property is held or owned by a criminal defendant or by a third party. Article 374 of the Penal Code calls for the confiscation of goods acquired through drug trafficking-related crimes and of any profit obtained. This allows for the confiscation of instruments and effects used for illegal drug dealing, as well as the goods or proceeds obtained from the illicit traffic.

A judge may impose provisional measures concerning seizures related to any type of offense by virtue of the code of criminal procedure. Effects may be seized and stored by the judicial authorities at the beginning of an investigation. The Fund of Seized Goods of Narcotics Traffickers, established under the National Drug Plan, receives seized assets. The proceeds from the funds are divided, with equal amounts going to drug treatment programs and to a foundation that supports officers fighting narcotics-trafficking. The division of assets from seizures involving more than one country depends on the relationship with the country in question. European Union (EU) working groups determine how to divide the proceeds for member countries. Outside of the EU, bilateral commissions are formed with countries that are members of FATF, FATF-style regional bodies (FSRBs), and the Egmont Group, to coordinate the division of seized assets. With other countries, negotiations are conducted on an ad hoc basis.

The banking community cooperates with enforcement efforts to trace funds and seize or freeze bank accounts. The law is unclear as to whether or not civil forfeitures are allowed. The GOS enforces existing drug-related seizure and forfeiture laws. The GOS has adequate police powers and resources to trace, seize, and freeze assets. Spain disseminates limited statistics on money laundering and terrorist financing investigations, prosecutions and convictions as well as on property frozen, seized and confiscated.

A small percentage of the money laundered in Spain is believed to be used for terrorist financing. It is primarily money from the extortion of businesses in the Basque region that is moved through the financial system and used to finance the Basque terrorist group ETA. After ETA announced the end of its cease-fire in June of 2007, reports of extortion against businesses located in the Basque and Navarra regions increased greatly. According to media reports, the estimated amount of money ETA successfully extorts is upwards of 900,000 euros (approximately $1,215,000) annually. Spain has long been dedicated to fighting terrorist organizations, including ETA, GRAPO, and more recently, al-Qaida. Spanish law enforcement entities have identified several methods of terrorist financing: donations to finance nonprofit organizations (including ETA and Islamic groups); establishment of publishing companies that print and distribute books or periodicals for the purposes of propaganda, which then serve as a means for depositing funds obtained through kidnapping or extortion; fraudulent tax and subvention collections; the establishment of “cultural associations” used to facilitate the opening of accounts and provide a cover for terrorist financing activity; and alternative remittance system transfers.

Crimes of terrorism are defined in Article 571 of the Penal Code, and penalties are set forth in Articles 572 and 574. Sanctions range from ten to thirty years’ imprisonment with longer terms if the terrorist actions were directed against government officials. On March 6, 2001, Spain’s Council of Ministers adopted a decision requesting the implementation of UNSCR 1373 in the Spanish legal framework. EU Council Regulation (EC) 881/2002 obliges covered countries such as Spain to execute UNSCR 1373. Terrorist financing issues are governed by a separate code of law and commission, the Commission of Vigilance of Terrorist Finance Activities (CVAFT). This commission was created under Law 12/2003 on the Prevention and Blocking of the Financing of Terrorism. Law 12/2003,

when implemented, will give the GOS the ability to freeze funds without going through the traditional judicial procedures, which some consider inefficient and burdensome, and will allow the GOS more latitude to freeze any type of financial flow so as to prevent the funds from being used to commit terrorist acts. However, the current GOS Administration has not enacted implementing regulations, and it appears there is no political will to do so. As with all EU countries, the obligation to freeze assets under UNSCR 1267 has also been implemented through the Council. Spain regularly circulates to its financial institutions the list of individuals and entities that have been included on the UN 1267 Sanctions Committee consolidated list. There were six actions taken against individuals or entities in 2005 under 1267 and/or 1373, for a total value of 83.75 euros (approximately $106). No assets associated with entities listed by the UN 1267 Sanctions Committee were reported to be in Spain in 2008.

Spain is a member of the FATF and co-chairs the FATF Terrorist Finance Working Group. Spain is also involved with FSRBs as an observer to the South American Financial Action Task Force and a cooperating and supporting nation to the Caribbean Financial Action Task Force. Spain is a major provider of AML/CTF assistance in Latin America. SEPBLAC is a member of the Egmont Group and currently chairs the Outreach Committee Working Group. Spain participates in the FIU.Net project for information exchange among European FIUs.

Spain actively collaborates with Europol, supplying and exchanging information on terrorist groups. In 2008, U.S. law enforcement agencies also reported excellent cooperation with their Spanish counterparts. Spanish media gave prominent coverage to the cooperation between the U.S. Drug Enforcement Administration (DEA) and Spanish law enforcement authorities that led to the August 12 joint DEA and Spanish National Police drug raid which resulted in the seizure of 1,400 kilos of cocaine and the arrest of six Colombian and Venezuelan nationals. In September 2007, Spanish police arrested two Pakistani men who were indicted in the U.S. on money laundering charges following a joint counterterrorism investigation with the Federal Bureau of Investigation. The investigation found evidence that more than 1 million euros (approximately $1,400,000) flowed from the drug trade and other criminal actions to terrorist groups. In September 2008, Agents from U.S. Immigration and Customs Enforcement (ICE) and officers from U.S. Customs and Border Protection (CBP) conducted a seven day joint bulk currency interdiction operation with Spanish Customs authorities. The operation, Hands Across the World (HAW), is an initiative targeting Bulk Cash Smuggling (BCS) worldwide. HAW was developed to fight BCS via real time intelligence sharing (including cash seizure/declaration data) between international law enforcement partners. The operation resulted in 13 seizures of U.S. and foreign currency totaling over $900,000.

The GOS has signed criminal mutual legal assistance agreements with Argentina, Australia, Canada, Chile, the Dominican Republic, Mexico, Morocco, Uruguay, and the United States. Spain's mutual legal assistance treaty with the United States has been in effect since 1993 and provides for sharing of seized assets "to the extent permitted by (domestic) laws." Spain has also entered into bilateral agreements for cooperation and information exchange on money laundering issues with 14 countries around the world, as well as with the United States. SEPBLAC has bilateral agreements for cooperation and information exchange on money laundering issues with more than 25 FIUs around the world.

Spain is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the UN Convention for the Suppression of the Financing of Terrorism.

The scale of money laundering and the sophisticated methods used by criminals represent a major threat to Spain. The Government of Spain should review the resources available for industry supervision, and ensure that SEPBLAC has the independence and resources it needs to effectively

discharge the duties entrusted to it. The GOS should work to close the loopholes in the areas of customer due diligence, beneficial ownership of legal persons, and the continued use of bearer shares. Spain should also work to implement Law 12/2003, which will greatly enhance Spain's capacity to combat terrorist financing. The GOS should clarify whether its laws allow civil asset forfeiture. Spain should maintain and disseminate statistics on investigations, prosecutions and convictions, including the amounts and values of assets frozen or confiscated. Spain should continue its efforts to actively participate in international fora and to assist jurisdictions with nascent or developing AML/CTF regimes.

St. Kitts and Nevis

St. Kitts and Nevis is a federation composed of two islands in the Eastern Caribbean. The federation is at major risk for corruption and money laundering due to the high volume of narcotics-trafficking activity through and around the island, and the presence of known traffickers on the islands. The growth of its offshore sector and an inadequately regulated economic citizenship program further contribute to the federation's money laundering vulnerabilities.

The Ministry of Finance oversees St. Kitts and Nevis' Citizenship by Investment Program. An individual may qualify for citizenship with a $350,000 minimum investment in real estate. In addition, the Government of St. Kitts and Nevis (GOSKN) created the Sugar Industry Diversification Foundation (SIDF), after the closure of the federation's sugar industry, as a special approved project for the purposes of citizenship by investment. To be eligible, an applicant must make a contribution ranging from $200,000 to $400,000 (based on the number of the applicant's dependents). The GOSKN requires applicants to make a source of funds declaration and provide evidence supporting the declaration. According to the GOSKN, the Ministry of Finance oversees the Citizenship Investment Program and has established a Citizenship Processing Unit to manage the screening and application process.

As a federation, there is anti-money laundering (AML), counterterrorist financing (CTF), and offshore legislation governing both St. Kitts and Nevis. However, each island has the authority to organize its own financial structure. With most of the offshore financial activity concentrated in Nevis, it has developed its own offshore legislation independently. As of October 2008, Nevis has one offshore bank, 109 licensed insurance companies, 13,257 international business companies (IBCs), 4,495 limited liability companies (LLCs), 1,001 international trusts, 70 multiform foundations (used for estate planning, charity financing, and special investment holding arrangements), and 40 registered agents. Figures from 2007 indicate St. Kitts has 1,592 exempt companies and foundations, nine exempt partnerships, 23 exempt trusts, 70 captive insurance companies, five trust service providers, 28 corporate service providers, and four licensed Internet gaming companies. Internet gaming entities must apply for a license as an IBC.

Bearer shares are permitted provided that bearer share certificates are retained in the safe custody of authorized persons or financial institutions authorized by the Minister of Finance as approved custodians. Legislation requires certain identifying information to be maintained about bearer certificates, including the name and address of the bearer as well as the certificate's beneficial owner. All authorized custodians are required by law to obtain proper documents on shareholders or beneficial owners before incorporating exempt or other offshore companies. This information is not publicly available but is only available to the regulator and other authorized persons.

The GOSKN licenses offshore banks and businesses. The GOSKN states that extensive background checks on all proposed licensees are conducted by a third party on behalf of the GOSKN before a license is granted. By law, all offshore bank licensees are required to have a physical presence in the federation; shell banks are not permitted. The Eastern Caribbean Central Bank (ECCB) has direct responsibility for regulating and supervising the offshore bank in Nevis, as it does for the entire

domestic sector of St. Kitts and Nevis, and for making recommendations regarding approval of offshore bank licenses. Under Section 10(8) of the Nevis Offshore Banking Ordinance, 1996, as amended in 2002, the ECCB is required to review all applications for licenses and report its findings to the Minister of Finance prior to consideration of the application.

The Proceeds of Crime Act No. 16 of 2000 (POCA) criminalizes money laundering for serious offenses (defined to include more than drug offenses), and imposes penalties ranging from imprisonment to monetary fines. The POCA overrides secrecy provisions that may have constituted obstacles to administrative and judicial authorities' ability to access information with respect to account holders or beneficial owners. The POCA was amended in April 2008 to include dealers in precious stones and metal in the list of regulated businesses for purposes of anti-money laundering/counterterrorist financing (AML/CTF). The POCA was amended in July 2008 to make money laundering an extraditable offence. The Money Services Business Bill 2008 seeks to provide for the licensing and regulation of the business of the transmission of money or monetary value in any form, which includes check cashing; currency exchange; and the issuance, sale or redemption of money orders or traveler's checks as well as the business of operating as an agent or franchise holder of any of these businesses.

The St. Kitts and Nevis Gaming Board is responsible for ensuring compliance by casinos. The Financial Services Commission (FSC) is the primary regulatory body for financial services in the federation and has the authority to cooperate with foreign counterparts on supervisory issues. Separate regulators for St. Kitts and Nevis carry out the actual supervision of institutions on behalf of the FSC, including AML examinations. Nevis seeks to consolidate its regulatory regime to a single unit, which would regulate all financial services businesses in Nevis, as of January 2009. This would expand supervision to credit unions, local insurance companies, and money transfer agencies. Nevis also seeks to establish a risk-based supervision program and will conduct risk assessments on all licensees, as well as establish a risk-based supervision schedule for onsite and offsite monitoring. The FSC has issued guidance notes on the prevention of money laundering, pursuant to the Anti-Money Laundering Regulations 2001. Regulations require financial institutions to identify their customers, maintain a record of transactions for up to five years, report suspicious transactions, and establish AML training programs. In July 2008, the GOSKN issued amended Anti-Money Laundering Regulations and Guidance Notes. The Regulations and Guidance Notes update and apply a risk-based approach to regulation and guidance, to include CTF measures; identification procedures for one-off transactions; and enhanced due diligence. A person who fails to comply with the requirements of these Regulations or Guidance Notes is liable on summary conviction to a fine not exceeding $50,000. In the case of a continuing offense, an additional fine of $5,000 per day is applicable for each day the infringement continues after such conviction.

The Financial Intelligence Unit Act No. 15 of 2000 (FIUA) authorizes the creation of a financial intelligence unit (FIU). The FIU began operations in 2001 and receives, collects, and investigates suspicious activity reports (SARs). All financial institutions, including nonbank financial institutions, are required by law to report suspicious transactions. AML regulations and the FIUA provide protection to reporting entities and employees, officers, owners, or representatives who forward SARs to the FIU. Tipping off is prohibited. The FIU has direct and indirect access to the records of other government entities via memorandums of understanding with domestic agencies. There is also indirect access to the records at financial institutions. The FIUA contains provisions for sharing information both domestically and with other foreign law enforcement agencies.

In 2008, the FIU received 352 SARs (triple the amount in 2007) with 98 referred to law enforcement for appropriate action. The FIU attributes this increase to efforts to increase awareness and educate entities of their reporting obligations. The GOSKN did not report any action taken on these referrals. The Royal St. Kitts and Nevis Police Force is responsible for investigating financial crimes, but does not have adequate staff or training to effectively execute its mandate.

The POCA limits and monitors the international transportation of currency and monetary instruments. Any person importing into or exporting from St. Kitts and Nevis a value exceeding $10,000 or its equivalent in Eastern Caribbean Currency needs to declare it through Customs. In addition, the Customs Control and Management Act criminalizes bulk cash smuggling. Customs and police share cash smuggling reports.

The Anti-Terrorism Act No. 21 of 2002 (ATA) provides the FIU and Director of Public Prosecutions the authority to identify, freeze, and/or forfeit terrorist finance-related assets. However, the law only allows for criminal forfeiture. Civil forfeiture is considered unconstitutional. Under the POCA, legitimate businesses can be seized by the FIU if proven to be connected to money laundering activities. The FIU and the Director of Public Prosecutions are responsible for tracing, seizing, and freezing assets. The FIU can freeze an individual's bank account for a period not exceeding five days in the absence of a court order. The freeze orders obtained via the court at times ascribe an expiration of six months or more. Also under the POCA, there is a forfeiture fund under the administration and control of the Financial Secretary in St. Kitts and the Permanent Secretary in the Ministry of Finance in Nevis.

The ATA criminalizes terrorist financing and implements various UN conventions against terrorism. The GOSKN circulates to its financial institutions the names of individuals and entities included on the UN 1267 Sanctions Committee's lists. The GOSKN has some existing controls that apply to alternative remittance systems, but has undertaken no initiatives that apply directly to the potential terrorist misuse of charitable and nonprofit entities. To date, no terrorist related funds have been identified.

The GOSKN has drafted the Non-Governmental Organization Bill and has had a first reading in the National Assembly. The main objective of the Bill is to regulate the operation of nongovernmental organizations (NGOs), including charities, and to stipulate that the registration of a NGO shall be refused if the entity or its proposed directors are involved or materially concerned in fraud, organized crime, money laundering or terrorist activities. The Bill also sets reporting standards intended to act as a monitoring mechanism for NGOs. It is anticipated the Bill will be passed before the end of 2008. All monies and proceeds from the sale of property forfeited or confiscated are placed in the fund to be used for AML activities in both St. Kitts and Nevis. Between 2001 and 2006, the GOSKN froze approximately $2,000,000 in assets, of which $1,000,000 was forfeited. No assets were seized in 2007 or 2008. In 2008, $154,000 was forfeited.

St. Kitts and Nevis is a member of the Caribbean Financial Action Task Force (CFATF), a Financial Action Task Force-style regional body, and underwent a mutual evaluation in 2008, the results of which are still pending. The mutual evaluation report will be presented at the CFATF Plenary in May 2009. St. Kitts and Nevis is also a member of the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD). The FIU is a member of the Egmont Group. St. Kitts and Nevis is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. St. Kitts and Nevis is not a party to the UN Convention against Corruption.

A Mutual Legal Assistance Treaty (MLAT) between the St. Kitts and Nevis and the United States entered into force in 2000. Past requests from the United States under the MLAT have not always been treated with appropriate responsiveness. . More recently, relations have improved, and there are efforts by the Director of Public Prosecutions office to remedy the previous deficiencies in the system. As a result of a refusal on the part of the GOSKN to remit over $1,000,000 in securities fraud proceeds arising out of a prosecution in the Southern District of California, the U.S. filed an action against the U.S. correspondent account of the Bank of Nevis under the USA PATRIOT Act in 2008. Recently, a judge in Nevis recognized the U.S. court-appointed SEC Receiver as an appropriate entity to receive

the fraud proceeds from the Bank of Nevis, and, as a result, as long as there is not a reversal of that decision, the U.S. action may be settled.

Bank secrecy laws, the allowance of anonymous accounts, and the lack of transparency of beneficial ownership of legal entities makes Nevis, in particular, a haven for criminals to conceal their proceeds. To address remaining vulnerabilities, St. Kitts and Nevis should devote sufficient resources to effectively implement its AML/CTF regime, giving particular attention to its offshore financial sector. It is also vital that St. Kitts and Nevis determine the exact number of Internet gaming companies present on the islands and provide the necessary oversight of these entities. As part of operating an offshore financial center, the Government of St. Kitts and Nevis needs to provide adequate resources and capacity to law enforcement agencies to effectively investigate money laundering cases. The GOSKN should provide for close supervision of its economic citizenship programs or else consider their discontinuance. Additionally, Nevis should expand its supervision program to credit unions, local insurance companies, and money transfer agencies. If it has not already done so, the GOSKN should enact its pending Money Services Business Bill 2008, to provide for licensing and supervision of money services businesses. To strengthen its legal framework against money laundering, St. Kitts and Nevis should move expeditiously to become a party to the UN Convention against Corruption.

St. Lucia

St. Lucia has developed an offshore financial service center that is vulnerable to money laundering. Transshipment of narcotics (cocaine and marijuana), unregulated money remittance businesses, cash smuggling, and bank fraud, such as counterfeit U.S. checks and identity theft, are among the other primary sources for laundered funds in St. Lucia.

Currently, St. Lucia has six offshore banks, 2,851 international business companies (IBCs), nine mutual funds, 29 international insurance companies, 66 trust companies, three mutual fund administrators, 15 registered agents, five registered trustees (service providers), and 30 domestic financial institutions. The number of IBCs reflects a 49 percent increase since 2006, though no information on the number of IBCs has been reported for 2008. Shell companies are not permitted. The Government of St. Lucia (GOSL) also has one free trade zone where investors may establish businesses and conduct trade and commerce within the free trade zone or between the free trade zone and foreign countries. There are no casinos or Internet gaming sites in St. Lucia, and the GOSL does not plan to consider the establishment of gaming enterprises.

Money laundering in St. Lucia is a crime under the 1993 Proceeds of Crime Act and the Money Laundering (Prevention) Act (MLPA) of 2003, which supersedes the Money Laundering (Prevention) Act of 1999 and the Financial Intelligence Authority Act of 2002. The MLPA criminalizes the laundering of proceeds with respect to numerous predicate offenses, including narcotics and firearms trafficking, abduction, blackmail, counterfeiting, extortion, forgery, corruption, fraud, prostitution, trafficking in persons, tax evasion, terrorism, gambling, illegal deposit taking and robbery. The MLPA mandates suspicious transaction reporting requirements and imposes record keeping requirements. In addition, the MLPA imposes a duty on financial institutions to take reasonable measures to establish the identity of customers, and requires accounts to be maintained in the true name of the holder. It also requires an institution to take reasonable measures to identify the underlying beneficial owner when an agent, trustee or nominee operates an account. These obligations apply to domestic and offshore financial institutions, including banks, building societies, financial services providers, credit unions, trust companies, and insurance companies. The Financial Services Supervision Unit has issued detailed guidance notes to implement the MLPA. Currently, steps are also being taken to implement legislation to regulate money remitters.

In 1999, the GOSL enacted a comprehensive inventory of offshore legislation, consisting of the International Business Companies (IBC) Act, the Registered Agent and Trustee Licensing Act, the

International Trusts Act, the International Insurance Act, the Mutual Funds Act, and the International Banks Act. An IBC may be incorporated under the IBC Act. Only a person licensed under the Registered Agent and Trustee Licensing Act as a licensee may apply to the Registrar of IBCs to incorporate and register a company as an IBC. IBCs intending to engage in banking, insurance or a mutual funds business may not be registered without the approval of the Minister responsible for international financial services. An IBC may be struck off the register on the grounds of carrying on business against the public interest.

The Committee on Financial Services, established in 2001, is designed to safeguard St. Lucia's financial services sector. The Committee is composed of, among others, the Minister of Finance, the Attorney General, the Solicitor General, the Director of Public Prosecutions, the Director of Financial Services, the Registrar of Business Companies, the Commissioner of Police, the Deputy Permanent Secretary of the Ministry of Commerce, the police officer in charge of the Special Branch, and the Comptroller of Inland Revenue. The GOSL has implemented administrative procedures for an integrated regulatory unit to supervise the currently regulated onshore and offshore financial institutions; however, the unit is not yet fully functional. The Eastern Caribbean Central Bank regulates St. Lucia's domestic banking sector.

The MLPA authorizes the establishment of St. Lucia's financial intelligence unit (FIU), which became operational in October 2003. The FIU is responsible for receiving, analyzing and disseminating suspicious transaction reports (STRs) from obligated financial institutions, and has regulatory authority to monitor compliance with anti-money laundering requirements. The FIU also is able to compel the production of information necessary to investigate possible offenses under the 1993 Proceeds of Crime Act and the MLPA. Failure to provide information to the FIU is a crime punishable by a fine or up to ten years imprisonment. The FIU has access to relevant records and databases of all St. Lucian government entities and financial institutions, and is permitted by law to share information with foreign FIUs. However, no formal agreement exists for sharing information domestically and with other FIUs. In 2008, the FIU received 56 STRs, two of which were referred to law enforcement agencies for further investigation. There are no recorded cases of money laundering within St. Lucia's banking sector for 2008.

Customs laws criminalize cash smuggling, and customs officials are aware of cash courier problems. Cash smuggling reports are shared with the FIU, police, Director of Public Prosecutions and the Attorney General.

Under current legislation, instruments of crime, such as conveyances, farms, and bank accounts, can be seized by the FIU. Substitute assets also can be seized. The legislation also applies to legitimate businesses if used to launder drug money, support terrorist activity, or if otherwise used in a crime. There is no legislation for civil forfeiture or sharing of narcotics assets. If the individual or business is not charged, then assets must be released within seven days. In 2008, $50,000 was frozen, while $350,000 was frozen in previous years.

The GOSL has not criminalized terrorist financing. However, St. Lucia circulates to financial institutions lists of terrorists and terrorist organizations on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to Executive Order 13224. The GOSL has the legislative power to freeze, seize and forfeit terrorist finance-related assets. To date, no accounts associated with terrorists or terrorist entities have been found in St. Lucia. The GOSL has not taken any specific initiatives focused on the misuse of charitable and nonprofit entities.

The GOSL has been cooperative with the USG in financial crimes investigations. In February 2000, St. Lucia and the United States brought into force a Mutual Legal Assistance Treaty.

The GOSL is a party to the 1988 UN Drug Convention; has signed, but not yet ratified, the UN Convention against Transnational Organized Crime; and is not a party to the UN Convention for the Suppression of the Financing of Terrorism or the UN Convention against Corruption. St. Lucia is a member of the Caribbean Financial Action Task Force, a Financial Action Task Force-style regional body, whose recent mutual evaluation report was made available in November 2008. The GOSL is also a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. St. Lucia's FIU is not a member of the Egmont Group.

The Government of St. Lucia should move expeditiously to criminalize terrorist financing. It also should enhance and implement its anti-money laundering legislation and programs by regulating money remitters, considering the adoption of civil forfeiture legislation and ensuring that its FIU meets the Egmont Group standards. Efforts to increase transparency within the island's offshore financial services sector should be continued. St. Lucia should also criminalize self-laundering and implement risk-based assessment procedures as well as consider requirements for reporting large monetary transactions to the FIU. The GOSL should intensify its efforts to investigate, prosecute, and sentence money launderers and those involved in other financial crimes, and should permit extradition in cases of money laundering and terrorist financing. St. Lucia should use its asset seizure and forfeiture regimes, and provide for asset sharing with other governments. Saint Lucia should become a party to the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption.

St. Vincent and the Grenadines

St. Vincent and the Grenadines (SVG) remains vulnerable to money laundering and other financial crimes as a result of drug-trafficking and its offshore financial sector. Money laundering is principally affiliated with the production and trafficking of marijuana in SVG, as well as the trafficking of other narcotics from South America. Money laundering occurs in various financial institutions such as domestic and offshore banks and money remitters. There has been a slight increase in fraud and the use of counterfeit instruments over the last year, such as tendering counterfeit checks or cash.

The domestic financial sector includes two commercial banks, a development bank, two savings and loan banks, a building society, nine insurance companies, ten credit unions, and two money remitters. The offshore sector includes six offshore banks, 8,498 international business corporations (IBCs), 13 offshore insurance companies, nine mutual funds, 19 registered agents, and 138 international trusts. There are no offshore casinos, and no Internet gaming licenses have been issued. There are no free trade zones in SVG. The Government of St. Vincent and the Grenadines (GOSVG) eliminated its economic citizenship program in 2001.

No physical presence is required for offshore sector entities and businesses, with the exception of offshore banks. Nominee directors are not mandatory except when an IBC is formed to carry on banking business. Bearer shares are permitted for IBCs but not for banks. The International Business Companies (Amendment) Act No. 26 and 44 of 2002 was enacted to immobilize bearer shares and requires registration and custody of bearer share certificates by a registered agent who must also keep a record of each bearer certificate issued or deposited in its custody. The record must contain pertinent information relating to the company issuing the shares, the number of the share certificate, and identity of the beneficial owner. The Offshore Finance Inspector has the ability to access the name or title of a customer account and confidential information about a customer that is in the possession of a license.

The Proceeds of Crime and Money Laundering (Prevention) Act 2001 (PCMLPA) criminalizes money laundering, and requires financial institutions and other regulated businesses to report suspicious transactions. Reporting is required for all suspicious activities regardless of the transaction amount. In 2005, the PCMLPA was amended to expand the definition to include an all offenses approach and to extend the scope of sections relating to the seizure, detention, and forfeiture of cash. The Proceeds of

Crime (Money Laundering) Regulations establish mandatory record keeping rules and customer identification requirements. Financial institutions are required to maintain all records relating to transactions for a minimum of seven years.

The Eastern Caribbean Central Bank (ECCB) supervises SVG's domestic banks. The International Banks (Amendment) Act No. 30 of 2002 provides the ECCB with enhanced authority to review and make recommendations regarding approval of offshore bank license applications, and to directly supervise the offshore banks in conjunction with the International Financial Services Authority (IFSA). The agreement includes provisions for joint on-site inspections to evaluate the financial soundness and anti-money laundering programs of offshore banks. However, in March 2008, an amendment to the International Bank Act was passed in Parliament. The amendment reduces the involvement of the ECCB in the supervision of the offshore banking sector. The IFSA continues independently to supervise and regulate other offshore sector entities; however, its staff exercises only rudimentary controls over these institutions. The GOSVG has strengthened the structure and staffing of the IFSA to regulate offshore insurance and mutual funds. The Exchange of Information Act No. 29 of 2002 authorizes and facilitates the exchange of information among regulatory bodies.

Customers are required to complete a source of funds declaration for any cash transaction over 10,000 East Caribbean dollars (XCD) (approximately $3,700). It is not mandatory to report other noncash transactions exceeding 10,000 XCD (approximately $3,700). Incoming travelers are required to declare currency over 10,000 XCD (approximately $3,700) on a customs declaration form, reintroduced in 2003.

The Financial Intelligence Unit Act No. 38 of 2001 (FIU Act) establishes the GOSVG's Financial Intelligence Unit (FIU). Operational as of 2002, the FIU has the mandate to receive, analyze, and investigate financial intelligence, and prosecute money laundering cases. Suspicious activity related to drug-trafficking is forwarded to the Narcotics Unit for further investigation, and activity related to fraud is forwarded to the Criminal Investigation Division. The FIU also has the ability to obtain production orders and stop/freeze orders. The FIU staff includes the director, financial investigators, legal officers, and administrative officers. As of November 2008, the FIU received 425 suspicious activity reports for the year, almost triple that of 2007. In December 2008, a suspect was arrested and charged under the Proceeds of Crime and Money Laundering Act. The charges relate to $1,700,000 which, in whole or in part, directly represent his proceeds of criminal conduct discovered within a harbor in St. Vincent on board a yacht owned by the suspect. Two other individuals, the operators of the vessel, were charged in April 2008, when the funds were discovered. The suspect's arrest is a major milestone for law enforcement in St. Vincent, as the first arrest under the Act.

The FIU is the main entity responsible for supervising and examining financial institutions for compliance with anti-money laundering and counterterrorist financing (AML/CTF) laws and regulations. The function is also performed by the IFSA and the ECCB. Money laundering controls also apply to nonbanking financial institutions and intermediaries, which the FIU monitors for compliance. Reporting entities that are fully cooperative with the FIU are protected by law. An amendment to the FIU Act permits the sharing of information even at the investigative or intelligence stage. The FIU does not have direct access to the records or databases of other government entities. Generally, records are still kept in physical form and must be retrieved manually.

Existing anti-money laundering legislation allows for the criminal forfeiture of intangible as well as tangible property. Drug-trafficking offenses may also be liable to the forfeiture provisions pursuant to the Drug (Prevention and Misuse) Act and the Criminal Code. There is no period of time during which the assets must be released. Frozen assets are confiscated by the FIU upon conviction of the defendant. Proceeds from asset seizures and forfeitures are placed by the FIU into the Confiscated Assets Fund established by the PCMLPA. Legitimate businesses can also be seized if used to launder drug money, support terrorist activity, or are otherwise used in a crime. A civil forfeiture bill has been drafted and is

currently before the National Anti-Money Laundering Committee (NAMLC) for its approval. In 2008, approximately $1,158,000 in assets and $729,000 in cash was frozen or seized. Of this amount, approximately $23,000 was forfeited.

In 2006, the GOSVG enacted the United Nations (Anti-Terrorism Measures) (Amendment) Act 2006, Act. No.13 (UNATMA). The UNATMA criminalizes terrorist financing and imposes a legal obligation on financial institutions and relevant businesses to report suspicious transactions relating to terrorism and terrorist financing to the FIU. The GOSVG circulates lists of terrorists and terrorist entities to all financial institutions in SVG. To date, no accounts associated with terrorists have been found. The GOSVG has not undertaken any specific initiatives focused on the misuse of charitable and nonprofit entities.

An updated extradition treaty and a Mutual Legal Assistance Treaty between the United States and the GOSVG entered into force in 1999. The FIU executes the Mutual Legal Assistance Treaty requests. A member of the Caribbean Financial Action Task Force (CFATF), a Financial Action Task Force-style regional body, the GOSVG was scheduled to undergo its second mutual evaluation in early 2008, but this was postponed. It is anticipated the evaluation will occur in 2009. The GOSVG is also a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering, and the FIU is a member of the Egmont Group. St. Vincent and the Grenadines is a party to the 1988 UN Drug Convention and the UN Convention for the Suppression of the Financing of Terrorism. St. Vincent and the Grenadines has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. St. Vincent and the Grenadines is not a party to the UN Convention against Corruption.

The Government of St. Vincent and the Grenadines has strengthened its AML/CTF regime through legislation and the establishment of an effective FIU. The GOSVG should continue to ensure this legislation is fully implemented, and the FIU has access to all necessary information. The GOSVG should insist the beneficial owners of IBCs are known and listed in a registry available to law enforcement, immobilize all bearer shares, and properly supervise and regulate all aspects of its offshore sector. The GOSVG should continue to provide training and devote resources to increase the cooperation among its regulatory, law enforcement, and FIU personnel in AML/CTF operations and investigations. To ensure timely and effective information sharing, the GOSVG would be well served by computerization of its record keeping systems. Passage of civil forfeiture legislation and broader use of special investigative techniques should be pursued to strengthen the government's anti-money laundering efforts. St. Vincent and the Grenadines should also become a party to the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Suriname

Suriname is not a regional financial center. Narcotics-related money laundering is closely linked to transnational criminal activity related to the transshipment of cocaine to the United States, Europe, and Africa. Domestic drug trafficking organizations and organized crime, with links to international groups, are thought to control much of the money laundering proceeds, which are "invested" in casinos, real estate, and private sector businesses. Additionally, money laundering occurs as a result of poorly regulated private sector activities, such as casinos and car dealerships, the nonbanking financial system (including money exchange businesses or "cambios"), and a variety of other means, including construction, the sale of gold purchased with illicit money, the purchase and sale of real estate, and the manipulation of commercial bank accounts.

Suriname is not an offshore financial center and has no free trade zones. There is a gold economy in the interior mining region of the country. Suriname has a significant informal economy, the majority of which is not linked to money laundering proceeds. Offshore banks and shell companies are not permitted in Suriname.

A package of legislation passed in 2002 included the criminalization of money laundering. The legislation, "Reporting of Unusual Transactions in the Provision of Services," addresses multiple issues related to all types of money laundering, including criminalizing money laundering, reporting of unusual transactions, and requiring service providers to request identification from each customer making a transaction. The legislation applies to both banking and nonbanking financial institutions.

The Central Bank of Suriname (CBS) is the sole monitoring authority for commercial banks; in that capacity the CBS supervises and examines financial institutions for compliance with anti money laundering legislation. The CBS is adequately staffed and trained for this purpose. Banking and nonbanking institutions are also required to report suspicious transactions to the Financial Intelligence Unit (FIU), which is under the authority of the Attorney General's Office.

Suriname's legislation requires that service providers confirm the identities of individual or corporate clients before completing requested services, and retain photocopies of identity documents and all other relevant documents pertaining to national and international transactions for a period of seven years.

Financial institutions are required to report suspicious transactions. In accordance with international standards, objective and subjective indicators have been approved to identify unusual transactions. An unusual transaction is defined as any transaction that deviates from the usual account, as well as any customer activities that are not "normal" daily banking business. Reporting is mandatory if financial transactions are above a certain threshold; however, sanctions for noncompliance are currently not enforced. The thresholds for financial institutions range from U.S. $5,000 for money-transfer offices to U.S. $10,000 for banks, insurance companies, money exchange offices, and savings and credit unions. Thresholds for nonbanking financial institutions and "natural legal persons" are U.S. $5,000 for casinos, U.S. $10,000 for dealers of precious metals and stones, and U.S. $25,000 for notaries, accountants, lawyers, and car dealerships.

The legislation includes a due diligence section that holds individual bankers responsible if their institution launders money and ensures confidentiality to bankers and others with respect to their cooperation with law enforcement officials.

Suriname's money laundering legislation provides for the establishment of the FIU. The FIU is an administrative body that performs analytical duties. Its responsibilities entail requesting, analyzing, and reporting to the Attorney General's Office information on unusual transactions or unusual transaction patterns that may constitute money laundering. If necessary, the FIU may request access to the records of other government entities. Bureaucracy and the lack of financial and human resources have made it difficult for the FIU to perform. Although the law requires financial institutions, nonbank financial institutions, and natural legal persons who provide financial services to report unusual transactions to the FIU, only approximately 130 entities in Suriname are registered with the FIU and have received information regarding Suriname's money laundering legislation. The FIU continues to have difficulty registering providers in certain sectors, and authorities reported that not all of Suriname's jewelers, notaries, credit unions, "cambios," casinos, or car dealers are aware of or in compliance with the requirements of the money laundering legislation. Furthermore, authorities expressed concern that service providers such as accountants, lawyers, and real estate brokers, are increasingly being hired by money launderers and should receive training in order to recognize and prevent money laundering. The only entities in full compliance with the law are the banking sector and the money-transfer offices. The FIU is not adequately staffed to both monitor unusual transactions and conduct outreach activities to ensure that all sectors are aware of and in compliance with the law to report unusual transactions. The number of unusual transaction reports reported to the FIU in 2008 was not available but government officials stated that there had been an approximate 20 percent increase in the number of reports in 2008 as compared to reports in 2007. The number of these reports that were investigated by law enforcement agencies was not available.

The Police Fraud Department and the Special Investigative Techniques section (BOT) of the Police Force are responsible for investigating financial crimes. To facilitate interagency coordination, Suriname has an Anti-Money Laundering Project Team, which consists of representatives from the FIU, Judicial Police, the Attorney General's Office, and the judiciary.

Suriname's anti-money laundering regime also includes a Financial Investigation Team (FOT) under the authority of the Judicial Police. The FOT is the body responsible for investigating all suspicious transactions identified by the FIU. Upon making a determination that an unusual activity report is indeed suspicious and sufficient to initiate an investigation, the FIU refers the matter to the Attorney General's Office. If the Attorney General's Office concurs with the determination, it directs the FOT to conduct an investigation. Prosecutors use evidence collected from FOT investigations to build legal cases. However, the FOT also suffers from a lack of personnel and resources that have rendered it largely ineffective over the past year. The 2004 sentencing of an individual to seven years imprisonment for intentional money laundering and for attempting to export a small amount of cocaine remains the most significant and longest money laundering sentence to date. Resource constraints and a severe shortage of judges are proving to be a limiting factor in expanding this success. Through the year, four new judges (two permanent and two substitutes) were sworn in; it remains to be seen if the expansion of the judges' corps will partially redress the problem.

There were two arrests and one prosecution for money laundering. In March 2008, two suspects were arrested on charges of money laundering after they were arrested carrying approximately U.S. $ 190,600. One of the suspects was still under prosecution at year's end, while the other, a government employee, was released without court charges and returned to his official duties.

In August 2008, a man originating from Sierra Leone, but residing in Suriname, was arrested for attempting to travel on a stolen passport. After his arrest, investigations led to seizure of his bank statements, which contained "thousands of U.S. dollars." The suspect could not properly explain the source of these funds. The Attorney General's Office was preparing charges against the suspect at year's end.

The appeal on the case involving De Surinaamse Bank President Siegmund Proeve, former Bank President Edward Muller, Procurement Officer Patrick Bhagwandin, and Canadian Dorsett Group staffer Jeffrey Clague continued in 2008. In August 2007, Proeve and Muller had been sentenced to six months imprisonment for the illegal transfer of approximately U.S. $14.5 million in casino profits to foreign countries between 1998 and 2003. The defendants were charged with transferring funds without the permission of the Foreign Exchange Commission, and for the transfer of amounts over U.S. $10,000 without reporting it to the Central Bank. Bagwandin was sentenced to a conditional three-month imprisonment, and Claque was sentenced to six months. The bank was fined U.S. $358,000. In October 2008, the Appeals Court reversed the ruling on Clague because he had not been properly served. The court is scheduled on December 15 to hand down a decision on whether or not Clague was legally required to submit capital lease documentation for the money transfers. The prosecution has asked the court to fine the DSB Bank 100,000 SRD (U.S. $35,714) and sentence Proeve and Muller to 12 months imprisonment.

The trial involving former Minister of Trade and Industry, Siegfried Gilds, continued at year's end. Gilds, who resigned his position after the Attorney General announced he was under investigation for laundering money and membership in a criminal organization, is alleged to have laundered close to $1.27 million between 2003 and 2005.

An amendment to the criminal code enacted in 2003 allows authorities to confiscate illegally obtained proceeds and assets obtained partly or completely through criminal offenses; however, assets cannot be converted to cash or disposed of until the case is settled. New assets forfeiture legislation, which would make this possible, is under consideration in Parliament. There are no provisions for civil forfeiture, and there is no legal mechanism that designates the proceeds gained by the sale of forfeited

goods to be used directly for law enforcement efforts. There is no entity for the management and disposition of assets seized and forfeited for narcotics-related money laundering offenses.

Suriname does have legislation that allows the authorities to freeze assets of those suspected of money laundering. The Police Fraud Department and the Special Investigative Techniques section (BOT) of the Police Force are responsible for investigating financial crimes and seizing assets. Assets may be confiscated pending the outcome of the trial, but cannot be liquidated until after the court's final verdict.

The government has not criminalized the financing of terrorism as required by the UN International Convention for the Suppression of the Financing of Terrorism, UN Security Council Resolution 1373, and FATF Special Recommendation Number 9. The Central Bank of Suriname circulates to commercial banks the names of individuals/entities that are designated by the United Nations 1267 Sanctions Committee list as associates of Al-Qaeda, the Taliban, or Usama bin Laden. The government has not adopted laws or regulations that allow for the exchange of records with the United States on investigations and proceedings related to terrorism and terrorist financing.

Suriname does not recognize indigenous alternative remittance systems. There are no known cases of charitable or nonprofit entities serving as conduits for financing terrorism in Suriname.

Statutory requirements limit the international transportation of currency and monetary instruments; amounts in excess of U.S. $10,000 must be reported to authorities before entering or leaving Suriname. In addition, any person who wishes to take money in excess of U.S. $10,000 out of the country must notify the Immigration Police. The Central Bank of Suriname also requires that all transactions in excess of U.S. $10,000 be reported. The GOS has not taken any strong action against cross-border cash smuggling and the extent of this smuggling is unknown. There is little publicly posted information at the borders or at the international airport on the requirement to report the transport of currency or monetary instruments in excess of U.S. $10,000. There is no database of cash declaration or smuggling reports.

Suriname has bilateral treaties and cooperation agreements with the United States on narcotics trafficking, and with Colombia, France and the Netherlands Antilles on transnational organized crime. There has been some cooperation with the United States on civil cases under U.S. jurisdiction. In January 2006, Suriname, the Netherlands Antilles, and Aruba signed a Mutual Legal Assistance Agreement allowing for direct law enforcement and judicial cooperation between the countries, making it no longer necessary for the process to be first routed through The Hague. Parties to the Agreement, which covers cooperation with regard to drug trafficking, trafficking in persons, and organized crime, had a follow-up meeting in March 2007 and expanded the cooperation to include information sharing on transnational crime and financial crimes. On the basis of a Memorandum of Understanding (MOU), Suriname shares information regarding money laundering with the FIU in the Netherlands. Another MOU was concluded with the Netherlands Antilles in October 2007.

Suriname is party to the 1988 UN Drug Convention, but has not implemented legislation regarding precursor chemical control provisions to bring itself into full conformity with the Convention. Suriname is a party to the UN Convention against Transnational Organized Crime but not a party to the UN Convention against Corruption. Draft legislation to become a party to the UN Convention for the Suppression of the Financing of Terrorism has been prepared by the Ministry of Justice and Police, and is awaiting the Council of Ministers' approval. Suriname is a member of the Caribbean Financial Action Task Force (CFATF) and the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Suriname's FIU is not a member of the Egmont Group. In 2006, a joint team from the FIUs of Canada and the United States visited Suriname and agreed to sponsor Suriname's FIU in the Egmont membership process. The two organizations proposed steps to be taken by Suriname to qualify for the Egmont application process. A crucial step

recommended is the formal criminalization of terrorist financing, which is a requirement for all new members of the Egmont Group.

The Government of Suriname should pass legislation to criminalize terrorist financing. Recent convictions have demonstrated the ability and willingness of the GOS to combat money laundering. However, the GOS should take steps to further enhance its anti-money laundering regime to conform to international standards. Suriname should devote the necessary resources to effectively investigate and prosecute money laundering cases. The GOS should consider implementing provisions for civil forfeiture, and create a program for the management and disposition of seized and forfeited assets. The GOS should bolster the capacity of the FIU with the necessary personnel and financial resources, and implement reforms to permit the FIU to qualify as a member of the Egmont Group. Suriname should become a party to the UN Convention against Corruption and to the UN Convention for the Suppression of the Financing of Terrorism, and pass the necessary laws to conform to its obligations under the 1988 UN Drug Convention.

Switzerland

Switzerland is a major international financial center. Reporting indicates that criminals attempt to launder illegal proceeds in Switzerland from a wide range of criminal activities conducted worldwide. These illegal activities include, but are not limited to, financial crimes, narcotics trafficking, arms trafficking, organized crime, terrorist financing and corruption. Although both Swiss and foreign individuals or entities launder money in Switzerland, foreign narcotics trafficking organizations, often based in the Balkans, Eastern Europe, or South America, dominate the narcotics-related money laundering operations in Switzerland. The country's central geographic location; relative political, social, and monetary stability; the range and sophistication of financial services it provides; and its long tradition of bank secrecy—first codified in 1934—not only contribute to Switzerland's success as a major international financial center, but also expose Switzerland to potential money laundering activity.

Given the size of the Swiss banking industry in the overall economy (with 330 banks and a large number of nonbank financial intermediaries comprising 11.8 percent of GDP, 5.9 percent of total employment, and 11.4 percent of total domestic revenues), Swiss authorities are aware of the vulnerabilities and have taken steps to mitigate them. For example, Switzerland automatically waives its bank secrecy laws in cases of suspected money laundering and fraud. Thus, while reference to Swiss bank accounts was once frequent in fraud and corruption cases linked to foreign government officials and heads-of-state, such cases are less common today. Swiss banks routinely screen the accounts of politically exposed persons (PEPs) for indications of illicit money transfers, making use of specialized computer software programs to monitor for suspicious activities. Examples of public figures that have been the subject of Swiss money laundering allegations or investigations include a former Kyrgyz Republic President, a former Russian Minister of Atomic Energy, the Nigerian dictator Sani Abacha, former Pakistani Prime Minister Benazir Bhutto, and former Haitian President Jean-Claude Duvalier. These individuals used Swiss bank accounts under the names of related family members to move national assets to Switzerland for personal use.

Switzerland's banking industry offers the same account services for both residents and nonresidents. Many Swiss banks offer certain well-regulated offshore services, including permitting nonresidents to form offshore companies to conduct business, which can be used for tax reduction purposes. However, Swiss commercial law does not recognize any offshore mechanism per se and its provisions apply equally to residents and nonresidents. The stock company and the limited liability company are two standard forms of incorporation offered by Swiss commercial law. All financial intermediaries must verify the identity of the beneficial owner of the stock company and must know any change regarding

the beneficial owner. Stock companies may issue bearer shares, but limited liability companies may not.

Switzerland has duty free zones. Customs authorities supervise the admission into and the removal of goods from customs warehouses. Warehoused goods may only undergo manipulations necessary for their maintenance, such as repacking, splitting, sorting, mixing, sampling and removal of the external packaging. Any further manipulation is subject to authorization. Goods may not be manufactured in the duty free zones. Swiss law has full force in the duty free zones. Export laws on strategic goods, war material, and medicinal products, as well as laws relating to anti-money laundering prohibitions, all apply.

Switzerland has no legal reporting requirement for cash imported into or exported out of the country. Because there are no laws meeting the international standards for declaration of currency and monetary instruments, Swiss authorities cannot effectively initiate bulk cash investigations.

Switzerland ranks third in the highly profitable global artwork trading market, exporting $1.8 billion of artwork in 2007—an increase of 41percent over the previous year. Because of the size of the Swiss art market, organized crime groups have attempted in the past to transfer stolen art or to use art to launder criminal funds via Switzerland. The United States is by far Switzerland's most important trading partner in this area, having purchased $576 million worth of works of art in 2007. This sum represents 31 percent of total artwork imports. The 2003 Cultural Property Transfer Act, implemented in June 2005, codifies in Swiss law elements of the 1970 United Nations Educational, Scientific, and Cultural Organization (UNESCO) Convention. This measure increases from five to thirty years the time period during which stolen pieces of art may be confiscated from those who purchased them in good faith. The law also allows police forces to search bonded warehouses and art galleries.

Switzerland has comprehensive anti-money laundering (AML) legislation in place, criminalizing money laundering and making banks and other financial intermediaries subject to strict know-your-customer (KYC) and reporting requirements. However, Swiss law does not recognize certain types of criminal offenses as predicate offenses for money laundering, including illegal trafficking in migrants, counterfeiting and pirating of products, smuggling, insider trading, and market manipulation. The fact that not all predicate crimes are covered under the money laundering laws increases the vulnerability of Switzerland's financial sector to criminal exploitation. In June 2007 the Swiss government submitted a draft bill to Parliament extending the scope of the Money Laundering Act to address shortcomings identified in the Financial Action Task Force (FATF) mutual evaluation report (MER) for Switzerland. The adoption of AML regulations planned for 2009 will make these crimes predicate offenses.

Swiss money laundering laws and regulations apply to both banks and nonbank financial institutions. The Federal Banking Commission, the Federal Office of Private Insurance, and the Swiss Federal Gaming Board serve as primary oversight authorities for a number of financial intermediaries, including banks, securities dealers, insurance institutions, and casinos. Other financial intermediaries are either directly supervised by Money Laundering Control Authority (MLCA) of the Federal Finance Department or by an accredited self-regulatory organization (SRO), which the entity must join. SROs are authorized by the Swiss government to oversee implementation of AML measures by their members. The SROs must be independent of the management of the intermediaries they supervise and must enforce compliance with due diligence obligations. Noncompliance can result in a fine or a revoked license. About 6,000 financial intermediaries are associated with SROs; the majority of these are financial management companies.

The Swiss Federal Banking Commission revised its AML regulations in 2002, and they became effective in 2003. These regulations, aimed at the banking and securities industries, codify a risk-based approach to suspicious transactions and client identification and install a global know-your-customer risk management program for all banks, including those with branches and subsidiaries abroad.

Consistent with this approach, financial intermediaries must conduct additional due diligence in the case of higher-risk business relationships. The regulations require increased due diligence in the cases of politically exposed persons (PEPs), ensuring that decisions to commence relationships with such persons be undertaken by at least one member of the senior executive body of a financial institution. All provisions apply to correspondent banking relationships as well. Swiss banks may not maintain business relationships with shell banks, but there is no requirement that banks ensure that foreign clients do not authorize shell banks to access their accounts in Swiss banks.

The 2002 Banking Commission regulations mandate that all cross-border wire transfers must contain identifying details about the funds' remitters, though banks and other covered entities may omit such information for "legitimate reasons." However, the MER states that Switzerland lacks specific provisions requiring intermediary financial institutions to keep the necessary information on the ordering customer.

In June 2007, the Swiss Parliament approved a new financial market regulation bill aimed at creating a new regulator to boost the image of Switzerland's financial market by combining the activities of three existing watchdog groups. The Federal Financial Market Supervisory Authority (FINMA) groups together the regulatory work of the Federal Banking Commission, the Federal Office of Private Insurance and the Money Laundering Control Authority. The FINMA became operational in January 2009, and will investigate suspected cases of money laundering and corruption.

Other types of designated nonfinancial businesses and professions (DNFBPs) required to report suspicious transactions to the Swiss FIU include attorneys, commodities and precious metals traders, asset managers and investment advisers, distributors of investment funds, securities traders, and credit card companies.

The Money Laundering Reporting Office (MROS), part of the Federal Office of Police (FedPol), is Switzerland's FIU and functions as a relay and filtration point between financial intermediaries and other law enforcement agencies. According to the Money Laundering Act, MROS receives, processes, and analyzes STRs, and disseminates them to law enforcement agencies. MROS cannot obtain additional information from reporting entities after receiving an STR. As an administrative FIU, MROS does not have any investigative powers of its own. From an operational standpoint, Swiss authorities claim that MROS has reached full capability, and that its experienced and efficient team has been able to keep average processing time to 2.5 days per STR.

MROS received 795 STRs in 2007, the most it has received since 2004. MROS forwarded seventy-nine percent of these STRs to law enforcement. The banking sector saw a 37 percent increase in the number of STRs submitted by its institutions. Of the total number of STRs, banks submitted 62 percent of STRs, followed by payment services with 29 percent of STR submissions, and money transmitters with 20 percent. The proportion of STRs that money transmitters submitted in 2007was half of that of previous years. According to Swiss authorities, one reason for the decrease in STRs from money transmitters was Swiss authorities' success interdicting various scams. While the DNFBP sectors submitted more STRs in 2007 than in 2006, their impact on the total reporting volume is relatively minor.

As was the case in the previous year, "fraud" was by far the most frequently suspected predicate offence (33 percent). In 2007, 6 STRs were related to terrorist finance, slightly fewer than the 8 STRs reported in 2006. After careful scrutiny, MROS forwarded only three of the six STRs to the Federal Prosecutor's Office, which later found that these also did not merit the initiation of criminal proceedings.

MROS has drawn criticism from fellow Egmont Group members that claim that MROS does not meet Egmont's definition that an FIU must have a formal legal basis to process STRs related to terrorist financing. However, Swiss law already refers to the MROS as a national reporting office for all

matters relating to the fight against terrorist financing. Because the Egmont Group still requires a formal legal basis for the MROS to meet all of the prerequisites for membership, Switzerland must amend Article 9-1 of the Anti-Money Laundering Act as proposed in the Federal Council's draft bill. If the procedure fails, the Swiss Justice Minister warned Parliament in October, the Egmont Group could suspend or cancel MROS' membership by April 2009.

Under the 2002 Efficiency Bill, the Swiss Attorney General has authority to prosecute crimes addressed by Article 340 of the Swiss Penal Code, which covers money laundering offenses. The law confers on the Federal Police and Attorney General's Office the authority to take over cases that have international dimensions, involve several cantons, or which deal with money laundering, organized crime, corruption, and white collar crime. Additional legislation increased the personnel and financing of the criminal police section of the Federal Police Office, which led to prosecutors' increased effectiveness pursuing organized crime, money laundering and corruption.

Switzerland has implemented legislation for identifying, tracing, freezing, seizing, and forfeiting assets. If financial institutions believe that assets derive from criminal activity, they must freeze the assets immediately until a prosecutor decides on further action. Under Swiss law, suspect assets may be frozen for up to five days while a prosecutor investigates the suspicious activity. Switzerland cooperates with the United States to trace and seize assets, and has shared large amounts of seized assets with the United States and other governments.

Switzerland has returned a total of $1.6 billion in illegal PEP assets to home countries. Most prominently, Switzerland returned $684 million in assets deposited by Ferdinand Marcos to the Philippines and $700 million in assets deposited by Sani Abacha to Nigeria. Historically, Switzerland has required court rulings in both Switzerland and the PEP's home country before returning the assets, but in Abacha's case, Switzerland returned the assets without a judgment from Nigeria. The Swiss government has indicated that two PEP cases, that of $6 million in assets deposited by Jean-Claude Duvalier of Haiti, and $8 million deposited by Mobuto Sese Seko of Congo, have been pending since 1986 and 1997, respectively. In October, Switzerland asked the Democratic Republic of Congo to provide judicial cooperation so that the money would not be returned to the Mobuto family.

The Swiss government has found it difficult occasionally to repatriate stolen financial assets to their countries of origin. Swiss authorities recognize the difficulties involved in obtaining court rulings from states without efficiently functioning judicial systems and point out that countries often fail to file legal assistance requests with Switzerland, or that internal politics of the requesting country has disrupted the legal proceedings. Switzerland is also considering how to work with countries which are unable, due to insufficient funds, to cooperate with the Swiss system of judicial review.

The Government of Switzerland (GOS) has worked closely with the USG on numerous money laundering cases. Swiss legislation permits "spontaneous transmittal," a process allowing the Swiss investigating magistrate to signal to foreign law enforcement authorities the existence of evidence regarding suspicious bank accounts in Switzerland. Six percent of the 1,510 foreign judicial assistance requests originated from the U.S. However, Swiss privacy laws make it extremely difficult for bank officials and Swiss police to divulge financial crime information to U.S. authorities absent a Mutual Legal Assistance Treaty (MLAT) request or Letters Rogatory.

Revisions to the Swiss Penal Code regarding terrorist financing entered into force on October 1, 2003. Article 260 of the Penal Code provides for a maximum sentence of five years' imprisonment for terrorist financing. Article 100 of the Penal Code, also added in 2003, extends criminal liability for terrorist financing to include companies. However, the Swiss Penal Code currently criminalizes the financing of an act of criminal violence, not the financing of an individual, independent of a particular act.

Swiss authorities regularly request that banks and nonbank financial intermediaries check their records and accounts against lists of persons and entities with links to terrorism. The entities must report accounts of these individuals and entities to the Ministry of Justice as suspicious. Along with the U.S. and UN lists, the Swiss Economic and Finance Ministries have drawn up their own list of individuals and entities they believe to be connected with international terrorism or its financing.

Swiss authorities have thus far blocked about 48 accounts totaling SFr. 25.5 million (approximately $20,648,360) from individuals or companies linked to individuals or entities listed pursuant to relevant UN resolutions. The Swiss Attorney General also separately froze 41 accounts representing about SFr. 25 million (approximately $22,943,800) on the grounds that they were related to terrorist financing, but the extent to which these funds overlap with the UN consolidated list has yet to be determined. As of October 2008, The State Secretariat for Economic Affairs (SECO) advised that 35 bank accounts totaling Sfr. 20 million (approximately $17,363,000) relating to Al-Qaeda and the Taliban remained frozen.

The last major investigation undertaken by the Federal Attorney General's Office on terrorism financing targeting the OFAC-listed Saudi Sheikh Yassin Kadi ended up as a defeat for Switzerland. In December 2007, authorities made the decision to abandon the prosecution, six years and two months after they began investigating the Saudi businessman whom the United States accused of supporting Al-Qaeda. As a result, the Swiss Attorney General is expected to unfreeze some 20 million francs (approximately $17,363,000) in several Swiss bank accounts.

Swiss authorities cooperate with counterpart bodies from other countries. Switzerland has a mutual legal assistance treaty in place with the United States, and Swiss law allows authorities to furnish information to U.S. regulatory agencies, provided it is kept confidential and used for law enforcement purposes. Switzerland is a member of the Financial Action Task Force (FATF), and its FIU is a member of the Egmont Group.

Switzerland is a party to the UN Convention for the Suppression of the Financing of Terrorism, the 1988 UN Drug Convention, and the UN Convention against Transnational Organized Crime. Switzerland has signed but not ratified the UN Convention against Corruption.

The Government of Switzerland (GOS) has been trying to correct the country's image as a haven for illicit banking services. The Swiss believe that their system of self-regulation, which incorporates a "culture of cooperation" between regulators and banks, equals or exceeds that of other countries. The Swiss strategy is to avert large risks by addressing them at the account-opening phase, where due diligence and know-your-customer procedures address the issues, rather than relying on an early-warning system on all filed transactions. The GOS should address the shortcomings identified in the FATF MER, including deficiencies in correspondent banking regulations and beneficial owner identification requirements. Switzerland should pass the enhanced regulations as planned, which will increase the number of predicate offenses for money laundering. Switzerland should enact and implement cross-border currency reporting requirements. Switzerland should also ratify the United Nations Convention against Corruption. The GOS should outlaw bearer shares completely, and implement effective AML legislation and rules that monitor and regulate money service businesses and the DNFBP sectors, including ensuring that the competent authorities have the resources to conduct outreach and complete their regulatory missions. Switzerland should ensure that FINMA has the proper resources to execute its work. Switzerland should also continue to explore measures regarding, and its work assisting, countries needing assistance for legal cooperation.

Syria

Syria is not an important regional or offshore financial center, due primarily to its still underdeveloped private banking sector and the fact that the Syrian pound is not a fully convertible currency. Despite

rapid growth in the banking sector since 2004, industry experts estimate that only eight percent of Syria's population of nearly 20 million people actually uses banking services. Consequently, some 70 percent of all business transactions are still conducted in cash. Additionally, there continue to be significant money laundering and terrorist financing vulnerabilities in Syria's financial and nonbank financial sectors that have not been addressed by legislation or other government action. Syria's black market moneychangers are not adequately regulated and the country's borders remain porous. Regional hawala networks are intertwined with smuggling and trade-based money laundering and raise significant concerns, including involvement in the financing of terrorism. The most significant indigenous money laundering threat involves Syria's political and business elite, whose corruption and extra-legal activities continue unabated. The U.S. Department of State has designated Syria as a State Sponsor of Terrorism.

The Syrian banking sector is dominated by the state-owned Commercial Bank of Syria (CBS), which holds approximately 75 percent of all deposits and controls most of the country's foreign currency reserves. With growing competition from private banks, CBS and the country's four other specialized public banks—the Agricultural Cooperative Bank, the Industrial Bank, the Real Estate Bank, and the People's Credit Bank—have begun offering a broader range of retail services to private customers. However, these state-owned banks still retain a monopoly on all government banking business, and account for some 80 percent of all bank branches nationwide.

In May 2004, the U.S. Department of the Treasury designated CBS, along with its subsidiary, the Syrian Lebanese Commercial Bank, as a financial institution of "primary money laundering concern," pursuant to Section 311 of The USA PATRIOT Act. This designation resulted from reports related to CBS's vulnerability to exploitation by criminal and/or terrorist enterprises, and has been used by terrorists or persons associated with terrorist organizations, as a conduit for the laundering of proceeds generated from the illicit sale of Iraqi oil. In April 2006, the U.S. Treasury promulgated a final rule, based on the 2004 designation, prohibiting U.S. financial institutions from maintaining or opening correspondent accounts with CBS or its Syrian Lebanese Commercial Bank subsidiary. These prohibitions also apply to foreign intermediary banks that have correspondent relationships with U.S. financial institutions and with CBS or its subsidiary.

The Government of Syria (GOS) began taking steps to develop a limited private banking sector in April 2001, with Law No. 28, which legalized private banking, and Law No. 29, which established rules on bank secrecy. Under Law No. 28, subsidiary branches of private foreign banks are required to have 51 percent Syrian ownership to be licensed in Syria. Bank of Syria and Overseas, a subsidiary of Lebanon's BLOM Bank, was the first private bank to open in Syria in January 2004. There are seven private, traditional banks in Syria, including Bank of Syria and Overseas (BSOM), Banque BEMO Saudi Fransi (French), the International Bank for Trade and Finance, Bank Audi, the Arab Bank, Byblos Bank, and Syria Gulf Bank. Four more traditional, private banks—the Bank of Jordan, the Orient Bank, Fransa Bank and Qatar National Bank—have obtained the necessary licenses and are expected to begin operations in Syria in 2009. In May 2005 a new law was enacted to allow for the establishment of Islamic banking. Al-Sham Islamic Bank began operations in August 2007. Additionally, Syria International Islamic Bank (IIB) opened its doors in September 2008. Al-Baraka Islamic Bank was also officially licensed in 2007.

By mid-2008, the Syrian banking sector reported assets totaling $34.3 billion and held deposits totaling $19.9 billion. Syrian banks are playing an increasing role in providing the business sector with foreign currency to finance imports and as a source of credit for businesses and individuals. However, the sector's development is hampered by the continuing lack of human expertise in finance, insufficient automation and communication infrastructure, regulations that limit Syrian banks' ability to make money on their liquidity, and restrictions on foreign currency transactions.

There are eight free trade zones in Syria, which are serviced mostly by subsidiaries of Lebanese banks, including Bank du Liban et d'Autre Mer, Banque Europeenne Pour le Moyen-Orient Sal, Bank of Beirut and Arab Countries, Bank Societee Generale, Fransa Bank, Societee du Banques Arabes, and Basra International Bank. In December 2007, the Central Bank of Syria ordered that these banks either cease operations or begin operating as branches of domestic (Syrian) banks within a period of six months. The Central Bank claimed that the move was necessary to standardize operating regulations for all banks across Syria. All free zone banks complied and operate as majority Syrian-owned subsidiaries of their parent banks. Four additional public free zones are planned for the cities of Homs, Dayr al Zur, Idleb, and the Port of Tartous. The Al-Ya'rubiyeh free zone in al-Hasakeh province, near the northeastern Syrian-Iraqi border, was officially inaugurated in December 2007.

In recent years, both China and Iran announced plans to build free zones in Syria, although Iran later dropped this idea in favor of pursuing a preferential trade agreement with Syria. China's free zone in Adra, however, was officially inaugurated in July 2008 and is expected to provide roughly 200 Chinese companies with a regional gateway for their goods. The volume of goods entering the free zones is estimated to be in the billions of dollars and is growing, especially with increasing demand for automobiles and automotive parts, which enter the zones free of customs tariffs before being imported into Syria. While all industries and financial institutions in the free zones must be registered with the General Organization for Free Zones, which is part of the Ministry of Economy and Trade, the Syrian General Directorate of Customs continues to lack strong procedures to check country of origin certification or the resources to adequately monitor goods that enter Syria through the zones. The importation and distribution of counterfeit goods are a concern. There are also continuing reports of Syrians using the free zones to import and export arms and other goods in violation of USG sanctions under the Syrian Accountability and Lebanese Sovereignty Restoration Act of 2003.

Legislation approved in the last few years provides the Central Bank of Syria with new authority to supervise the banking sector and investigate financial crimes. In September 2003, the GOS passed Decree 59, which criminalized money laundering and created an Anti-Money Laundering Commission (Commission) in May 2004. In response to international pressure to improve its anti-money laundering and counterterrorist financing (AML/CTF) regulations, the GOS passed Decree 33 in May 2005, which criminalized the act of terrorist financing and strengthened the Commission empowering it to act as a Financial Intelligence Unit (FIU). The Decree finalized the Commission's composition to include the Governor of the Central Bank, a Supreme Court Judge, the Deputy Minister of Finance, the Deputy Governor for Banking Affairs, and the GOS's Legal Advisor, and will include the Chairman of the Syrian Stock Market once the market is operational. However, the 2006 Middle East and North Africa Financial Action Task Force (MENAFATF) Mutual Evaluation rated the FIU as partially compliant, citing the lack of outreach to financial institutions and banks regarding the reporting of suspicious transaction reports, issues with budgetary independence, weak information protection controls, and overall efficiency.

Decree 33 provides the Commission with a relatively broad definition of what constitutes a crime of money laundering, but one that does not fully meet international standards set by the FATF. The definition includes acts that attempt to conceal the proceeds of criminal activities, the act of knowingly helping a criminal launder funds, and the possession of money or property that resulted from the laundering of criminal proceeds. In addition, the law specifically lists thirteen crimes that are covered under the AML legislation, including narcotics offenses, fraud, and the theft of material for weapons of mass destruction. Terrorist financing is not considered a predicate offense for money laundering crime or otherwise punishable under Decree 33. The act of terrorist financing criminalized by Decree 33 also fails to cover the intention that funds should be used or the knowledge that funds are to be used, in full or in part, by a terrorist organization or an individual terrorist in accordance with international standards.

Under Decree 33, banks and nonfinancial institutions are required to file reports with the Commission for transactions over the equivalent of $10,000, as well as suspicious transaction reports (STRs) regardless of amount. However, there is no obligation for financial institutions to report STRs related to terrorist financing or attempts to conduct suspicious transactions. Institutions are also required to use "know your customer" (KYC) procedures to follow up on their customers every three years and maintain records on closed accounts for five years. The chairmen of Syria's private banks continue to report that they are employing internationally recognized KYC procedures to screen transactions and also employ their own investigators to check suspicious accounts. Nonbank financial institutions must also file STRs with the Commission, but many of them continue to be unfamiliar with the requirements of the law. The Commission has organized workshops for these institutions over the past three years, but more time is needed for the information to penetrate the market.

Once a STR has been filed, the Commission has the authority to conduct financial investigations, waive bank secrecy on specific accounts to gather additional information, share information with the police and judicial authorities, and direct the police to carry out a criminal investigation. In addition, Decree 33 empowers the Governor of the Central Bank, who is the chairman of the Commission, to share information and sign Memoranda of Understanding (MOUs) with foreign FIUs. In November 2005, the Prime Minister announced that the Commission had completed an internal reorganization, creating four specialized units to: oversee financial investigations; share information with other GOS entities including customs, police and the judiciary; produce AML/CTF guidelines and verify their implementation; and develop a financial crimes database.

While a STR is being investigated, the Commission can freeze accounts of suspected money launderers for a nonrenewable period of up to eighteen days. The law also stipulates the sanctions for convicted money launderers, including a three to six-year of imprisonment and a fine that is equal to or double the amount of money laundered. Further, the law allows the GOS to confiscate the money and assets of the convicted money launderer. The Commission circulates among its private and public banks the names of suspected terrorists and terrorist organizations listed on the UNSCR 1267 Sanction Committee's consolidated list. It has taken action to freeze the assets of designated individuals, but has not frozen the assets of any Syrian citizens in 2008.

In 2008, the Commission investigated 137 cases involving suspicious transactions, 18 of which were forwarded by foreign jurisdictions. Twenty of these cases were referred to the criminal court system for prosecution. Over the past four years, the Commission has investigated 493 cases and referred 78 of them to the criminal court system. To date, all criminal cases remain pending, and there have been no convictions. Most Syrian judges are not yet familiar with the evidentiary requirements of the law. Furthermore, the slow pace of the Syrian legal system and political sensitivities delay quick adjudication of these issues. The Commission itself continues to be seriously hampered by human resource constraints, although it has increased its staff from six in 2005 to ten in 2008, and hopes to expand to 30 by the end of 2009. Nevertheless, a lack of local expertise—further undermined by a lack of political will—continues to impede effective implementation of existing AML/CTF regulations in Syria.

The GOS has not updated its laws regarding charitable organizations to include strong AML/CTF language. A promised updated draft law is still pending. The GOS decided at the end of 2004 to restrict charitable organizations to only distributing nonfinancial assistance, but the current laws do not require organizations to submit detailed financial information or information on their donors. While the Commission says that it is seeking to increase cooperation with the Ministry of Social Affairs and Labor, which is supposed to approve all charitable transactions, this remains a largely unregulated area.

Although Decree 33 provides the Central Bank with the legal basis to combat money laundering, most Syrians still do not maintain bank accounts or use checks, credit cards, or ATM machines. The Syrian

economy remains primarily cash-based. Syrians use moneychangers, some of whom also act as hawaladars, for many financial transactions. Estimates of the volume of business conducted in the black market by Syrian moneychangers range between $15-$70 million per day. (The GOS admits that it does not know the amount of money that is in circulation.) The GOS has begun issuing new regulations to entice people to use the banking sector, including offering high interest certificates of deposit and allowing Syrians to access more foreign currency from banks when they are traveling abroad. In 2006, the GOS passed a Moneychangers Law requiring that moneychangers be licensed. However, there were significant delays in the issuance of implementation instructions. To date, 25 moneychangers have applied for licensing, and just ten are now operating legally. The Commission does have the authority to monitor the sector under Decree 33, but the GOS has not yet begun investigating illegal money-changing operations. Consequently, hawaladars in Syria's black market remain a source of concern for money laundering and terrorist financing.

While the GOS maintains strict controls on the amount of money that individuals can take with them out of the country, there is a high incidence of cash smuggling across the Lebanese, Iraqi, and Jordanian borders. Most of the smuggling involves the Syrian pound, as a market for Syrian currency exists among expatriate workers and tourists in Lebanon, Jordan, and the Gulf countries. U.S. dollars are also commonly smuggled in the region. Some of the smuggling may involve the proceeds of narcotics and other criminal activity. In addition to cash smuggling, there also is a high rate of commodity smuggling, particularly of diesel fuel, prompted by individuals buying diesel domestically at the low subsidized rate and selling it for much higher prices in neighboring countries. The regional smuggling of stolen cars, counterfeit goods and cigarettes are also areas of concern. There are reports that some smuggling is occurring with the knowledge of or perhaps even under the authority of the Syrian security services.

The General Directorate of Customs lacks the necessary staff and financial resources to effectively handle the problem of smuggling. And while it has started to enact some limited reforms, including the computerization of border outposts and government agencies, problems of information-sharing remain. In September 2006, the Minister of Finance issued a decision stipulating the establishment of a unit specializing in AML/CTF within the General Directorate of Customs. Customs also lacks the infrastructure to effectively monitor or control even the legitimate movement of currency across its borders. The Commission and Customs have reportedly implemented a form asking individuals to voluntarily declare currency when entering or exiting the country, although consistency of implementation and any action resulting from enforcement are unknown. These shortfalls pose terrorist financing and money laundering vulnerabilities through trade-based money laundering and cash-based smuggling.

The Syrian FIU is a member of the Egmont Group of FIUs. In 2008, the Commission signed cooperation agreements and memoranda of understanding with the FIUs of Turkey and the Ukraine. These memoranda covered money laundering and terrorism financing. Syria is a member of the MENAFATF.

Syria and the United States do not have a mutual legal assistance agreement in place. Syria is a party to the 1988 UN Drug Convention and in April 2005, it became a party to the International Convention on the Suppression of the Financing of Terrorism. It has signed, but not yet ratified, both the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. Syria is ranked 147 out of 180 countries on Transparency International's 2008 Corruption Perception Index.

While the Government of Syria has made modest progress in implementing AML/CTF regulations that govern its formal financial sector, the continuing lack of transparency of the state-owned banks and their vulnerability to political influence reveals an absence of political will to address AML/CTF in the largest part of the banking sector. In addition, nonbank financial institutions and the black market continue to be vulnerable to money laundering and terrorist financing. To build confidence in

Syria's intentions, the Central Bank should be granted independence and supervisory authority over the entire sector. To enhance the implementation of Syria's AML/CTF legislation and private sector internal controls, the GOS should strengthen and train its FIU and should also grant it a degree of independence. Additionally, Syria should continue to modify its AML/CTF legislation and enabling regulations so that they adhere to international standards. The General Directorate of Customs, the Central Bank, and the judicial system in particular continue to lack the resources and the political will to effectively implement AML/CTF measures. Although the GOS has stated its intention to create the technical foundation through which different government agencies could share information about financial crimes, this mechanism still does not exist. Syria's shortfalls in its anti-terrorist financing controls poses grave threats given that U.S. designated foreign terrorist organizations, including HAMAS, Palestinian Islamic Jihad (PIJ), the Popular Front for the Liberation of Palestine (PLFP), and the Popular Front for the Liberation of Palestine-General Command (PFLP-GC), among others, all have offices in Damascus and operate within Syria's borders. Syria's provision of safe haven for these groups poses significant terrorist financing risks to both the Syrian and regional financial sectors. It remains doubtful that the GOS has the political will to punish terrorist financing or to address the corruption that exists at the highest levels of government and business. All of these issues remain obstacles to developing a comprehensive and effective AML/CTF regime in Syria. Syria should become a party to the UN Convention against Transnational Organized Crime and the UN Convention against Corruption.

Taiwan

Taiwan's modern financial sector and its role as a hub for international trade make it susceptible to money laundering. Taiwan's location astride international shipping lanes makes it vulnerable to transnational crimes, such as narcotics trafficking, trade fraud, and smuggling. There has traditionally been a significant volume of informal financial activity through unregulated nonbank channels, but in recent years Taiwan has taken steps to shift much of this activity into official, regulated financial channels. In November 2008 China and Taiwan reached an agreement to facilitate direct remittances across the Taiwan Strait. Taiwan will now allow direct remittances from China as of February 16, 2009. For remittances to China, Taiwan is allowing a growing number of postal savings outlets to provide this service. Most illegal or unregulated financial activities are related to tax evasion, fraud, or intellectual property violations. According to suspicious activity reports (SARs) filed by financial institutions on Taiwan, the predicate crimes most commonly linked to SAR reporting include financial crimes, corruption, and other general crimes.

Taiwan's anti-money laundering legislation is embodied in the Money Laundering Control Act (MLCA) of April 23, 1997, which was amended in 2003, 2007, and 2008. Its major provisions include a list of predicate offenses for money laundering, customer identification and record keeping requirements, disclosure of suspicious transactions, international cooperation, and the creation of a financial intelligence unit (FIU), the Money Laundering Prevention Center (MLPC).

The MLPC, a law enforcement-style FIU, is located within the Ministry of Justice Investigation Bureau (MJIB). The FIU receives, analyzes, and disseminates suspicious transaction reports, currency transaction reports and cross-border currency movement declaration reports. The MLPC also assists other law enforcement authorities to investigate money laundering and terrorist financing cases. MLPC staff has law enforcement status.

The 2003 amendment expanded the list of predicate crimes for money laundering, widened the range of institutions subject to suspicious transaction reporting, and mandated compulsory reporting to the MLPC of significant currency transactions in excess of New Taiwan dollars (NT $) 1 million (approximately U.S. $29,600). The Asia/Pacific Group on Money conducted a mutual evaluation of Taiwan in 2007. Following the recommendation of the mutual evaluation report (MER), in November

2008 the Financial Supervisory Commission changed the requirements to include transactions in excess of NT$500,000 ($14,800) to be reported. These amounts are comparable to levels for Singapore and Hong Kong. In 2007, the MLPC received 1,190,753 currency transaction reports. The 2003 amendments further expanded the scope of reporting entities beyond traditional financial institutions to include: automobile dealers, jewelers, boat and aviation dealers, real estate brokers, credit cooperatives, consulting companies, insurance companies, and securities dealers.

In July 2007, the MLCA was amended to expand its coverage to include a new agricultural bank, trust companies, and newly licensed currency exchanges as well as hotels, jewelry stores, postal offices, temples, and bus/railway stations, essentially all entities that may be involved in currency exchange. The list of predicate offenses was expanded to include offenses against the Public Procurement Law, Bills Finance Management Law, Insurance Law, Financial Holding Company Law, Trust Law, Credit Cooperative Association Law, and Agriculture Financing Law. The number of agencies with money laundering responsibilities was expanded from the Ministry of Justice, the Ministry of Transportation and Communication, and the Ministry of Finance to include also the Financial Supervisory Commission (established in July 2004), the Ministry of Economic Affairs, the Council of Agriculture (supervising a new agriculture bank and the credit departments of farmers' and fishermen's associations), and Taiwan's Central Bank (monitoring currency exchanges). The amended law also authorized Taiwan agencies to share information obtained from the MLCA with law enforcement agencies in countries that have signed a mutual legal assistance agreement (MLAA) with Taiwan and on a reciprocal basis with other countries. Following the MER recommendations the MCLA was again amended in June 2008 to include embezzlement from business firms in the list of major crimes subject to money laundering regulation.

Taiwan established a single financial regulator, the Financial Supervisory Commission (FSC) on July 1, 2004. The FSC consolidates the functions of regulatory monitoring for the banking, securities, futures and insurance industries, and also conducts financial examinations across these sectors. In mid-December 2005, the FSC began an incentive program for the public to provide information on financial crimes. The reward for information on a financial case with fines of NT $10 million (approximately $290,000) or at least a one-year sentence is up to NT $500,000 (approximately $14,800). The reward for information on a case with a fine of between NT $2 million and $10 million (approximately $58,000 and $290,000) or less than a one-year sentence is up to NT $200,000 (approximately $5,900).

Two new articles added to the 2003 amendments to the MLCA grant prosecutors and judges the power to freeze assets related to suspicious transactions and give law enforcement more powers related to asset forfeiture and the sharing of confiscated assets. The 2007 amendment to the MLCA permits the freezing of proceeds of money laundering for up to one year. In terms of reporting requirements, financial institutions are required to identify, record, and report the identities of customers engaging in significant or suspicious transactions. There is no threshold amount specified for filing suspicious transaction reports. The time limit for reporting cash transactions of over NT $1 million (approximately $29,600) is five business days. Banks are barred from informing customers ("tipping off") that a STR has been filed. Reports of suspicious transactions must be submitted to the MLPC within 10 business days. In 2007, the MLPC received 1,741 STRs and 31 of them resulted in prosecutions based on the MLCA. Of these 31 cases, nineteen are related to financial crimes, four to corruption, one to narcotics, and seven to other miscellaneous crimes. This represents a significant drop from prior years due to a change in the MLCA in mid 2007, which called for only cases involving amounts in excess of NT$ 1 million (approximately $29,600) to be handled under the MLCA. The rest are handled under other laws. A total number of 1,190, 755 Cash Transaction reports (CTRS) were filed by financial institutions in 2007. Additionally, as recommended in the MER, the threshold for occasional cash transactions that triggers a Customer Due Diligence (CDD) obligation

and CTR obligation was lowered from NT$1 million (approximately $29,600) to NT$ 500,000 (approximately $ 14,800)

As recommended in the MER, Taiwan Customs was required to start reporting foreign currencies and negotiable securities, including bearer shares, carried by passengers in excess of U.S. $10,000. The number of such cases reported to the MLPC in 2007 was 5,157, including 2,654 outbound involving NT$6,928.4 million (U.S. $210 million) and 2,503 inbound involving NT$6,460 million (U.S. $196 million). Customs also became a member of the Customs Asia Pacific Enforcement Reporting System and has signed MOUs with counterparts in the U.S., Australia, and the Philippines for sharing customs information.

Institutions are also required to maintain records necessary to reconstruct significant transactions. Bank secrecy laws are overridden by anti-money laundering legislation, allowing the MLPC to access all relevant financial account information. Financial institutions are held responsible if they do not report suspicious transactions. In May 2004, the Ministry of Finance issued instructions requiring banks to demand two types of identification and to retain photocopies of the identification presented when bank accounts are opened on behalf of a third party, to prove the true identity of the account holder. Individual bankers can be fined NT $200,000 to $1 million (approximately U.S. $6,060 to $30,300) for not following the provisions of the MLPA. Starting in August 2006, the Financial Supervisory Commission required banking institutions to collect, verify and store information about any banking customer who makes any single cash or electronic remittance above NT $30,000 (approximately U.S. $ 890).

All foreign financial institutions and offshore banking units follow the same regulations as domestic financial entities. Offshore banks, international businesses, and shell companies must comply with the disclosure regulations from the Central Bank, the Banking Bureau of the Financial Supervisory Commission, and MLPC. These supervisory agencies conduct background checks on applicants for banking and business licenses. Offshore casinos and Internet gambling sites are illegal. According to the Central Bank, as of September 2008, Taiwan hosted 31 local branches of foreign banks, one trust and investment company, and 63 offshore banking units.

On January 5, 2006, legislation was ratified to allow expansion of offshore banking unit (OBU) operations to the same scope as Domestic Business Units (DBU). This was done to assist China-based Taiwan businesspeople in financing their business operations. DBUs engaging in cross-strait financial business must follow the regulations of the “Act Governing Relations between Peoples of the Taiwan Area and the Mainland Area” and “Regulations Governing Approval of Banks to Engage in Financial Activities between the Taiwan Area and the Mainland Area.” The Competent Authority,” as referred to in these Regulations, is the Financial Supervisory Commission (FSC).

Taiwan prosecuted 31 cases involving money laundering in 2007, compared with 689 cases involving financial crimes in 2006. Among the 31 cases, nineteen involved unregistered stock trading, credit card theft, currency counterfeiting or fraud. Among the twelve other money laundering cases, four were corruption-related and one was drug-related. In July 2007, the MCLA was amended so that only cases involving amounts exceeding NT $5 million (approximately $148,000) were covered under the MLCA, while the rest were handled in accordance with other laws. The number of indicted subjects in 2007 was 122 persons. Figures are not yet available for 2008.

To comply with Financial Action Task Force (FATF) Special Recommendation Nine on bulk cash smuggling, the July 2007 legislation required individuals to report currency transported into or out of Taiwan in excess of NT $60,000 (approximately $1,780), U.S. $10,000 in foreign currency, 20,000 Chinese Yuan (approximately $2,930), or gold worth more than $20,000. When foreign currency in excess of NT $500,000 (approximately $14,800) is transferred into or out of Taiwan via the Taiwan banking system, the transfer must be reported to the Central Bank, though there is no requirement for Central Bank approval prior to the transaction. Prior approval is required, however, for exchanges

between New Taiwan dollars and foreign currency when the amount exceeds $5 million for an individual resident or $50 million for a corporate entity. Those who transfer funds over NT $30,000 (approximately $890) at any bank in Taiwan must produce a photo ID, and the bank must record the name, ID number and telephone number of the client.

Prior INSCR reports indicated that a "Counter-Terrorism Action Law" had been pending with the Legislative Yuan since 2003 which would explicitly designate the financing of terrorism as a major crime and give law enforcement agencies broad powers to seize suspected terrorist assets without a criminal case. In emergencies, they could also freeze assets for up to three days without a court order. The current administration, which came into office in 2008, has put forward new legislation which would provide less sweeping police powers. Financing of terrorist activities in Taiwan is already a criminal office under Taiwan law, but the draft law would extend the law to explicitly criminalize financing and money laundering in support of such activities overseas.

Although Taiwan does not criminalize terrorist financing as an autonomous offense, under the MLCA Taiwan officials currently have the authority to freeze and/or seize terrorist-related financial assets. Under the Act, the prosecutor in a criminal case can initiate freezing assets, or without criminal charges, the freezing/seizure can be done in response to a request made under a treaty or international agreement. The Banking Bureau of the FSC circulates the names of individuals and entities included on the UN 1267 Sanctions Committee's consolidated list, as well as names designated by the U.S. Treasury, to all domestic and foreign financial institutions and relevant government agencies. Banks are required to file a report on cash remittances if either of the parties involved are on a terrorist list. Although, as noted above, Taiwan does not yet have the authority to confiscate the assets, the MLCA was amended to allow the freezing of accounts suspected of being linked to terrorism.

Alternative remittance systems, or underground banks, are considered to be operating in violation of Banking Law Article 29. Authorities in Taiwan consider these entities to be unregulated financial institutions. Foreign labor employment brokers, after obtaining a permit from the Central Bank, are authorized to act on the behalf of foreign workers to use banks to remit income earned by foreign workers to their home countries. These brokers may not start the remittance services before they obtain a bank guarantee for the involved funds. They are required to sign and retain a standard remittance service contract with foreign workers and establish remittance records for each contracting foreign worker. There were 39 foreign labor employment brokers as of October 2008. If brokers accept money in Taiwan dollars for delivery overseas in another currency, they are violating Taiwan law. It is illegal for retail outlets to accept money in Taiwan dollars and remit it overseas. Violators are subject to a maximum of three years in prison, and/or forfeiture of the remittance, and/or a fine equal to the remittance amount.

Authorities in Taiwan do not believe that charitable and nonprofit organizations in Taiwan are being used as conduits for financing terrorism. Such organizations are required to register with the government and, like any other individual or corporate entity, are checked against a list of names designated by the United Nations or the U.S. Treasury as being involved in terrorist financing activities. The Ministry of Interior (MOI) is in charge of overseeing foundations and charities. Every three years the MOI assigns public accountants to audit the financial statements and also has management specialists assess the overall operations of nationally-chartered foundations.

Article 3 of Taiwan's Free Trade Zone Establishment and Management Act defines a Free Trade Zone (FTZ) as a controlled district of an international airport or an international seaport approved by the Executive Yuan. The FTZ coordination committee, formed by the Executive Yuan, has the responsibility of reviewing and examining the development policy of the FTZ, the demarcation and designation of FTZs, and inter-FTZ coordination.

There are five FTZs in Taiwan, all of which have opened since 2004, including the Taipei Free Trade Zone, the Taichung Free Trade Zone, the Keelung Free Trade Zone, the Kaohsiung Free Trade Zone, and the Taoyuan Air Cargo Free Trade Zone. These FTZs were designated with different functions, so that Keelung and Taipei FTZs focus on international logistics; Taoyuan FTZ on high value-added industries; Taichung FTZ on warehousing, transshipment and processing of cargo; and Kaohsiung FTZ on mature industrial clusters. According to the Center for Economic Deregulation and Innovation (CEDI) under the Council for Economic Planning & Development, as of November 2007 there were thirteen shipping and logistics companies listed in the Kaohsiung Free Trade Zone, 21 logistics companies in Taichung Free Trade Zone, five logistics and shipping companies in Keelung Free Trade Zone, two logistics companies in Taipei Free Trade Zone, and ten logistics and shipping companies and 24 manufacturers in Taoyuan Air Cargo Free Trade Zone. Shipments through these FTZs in 2007 surged 289 percent to NT$ 59.9 billion (approximately $1.7 billion), and the value of shipments in the first nine months of 2008 was NT$ 86.6 billion ($2.57 billion). While these increases are in indeed sizeable, this accounts for only 0.65 percent of Taiwan's two-way trade in the same period.

There is no indication that FTZs in Taiwan are being used in trade-based money laundering schemes or by the financiers of terrorism. According to Article 14 of the Free Trade Establishment and Management Act, any enterprise applying to operate within an FTZ shall apply to the management authorities of the particular FTZ by submitting a business operation plan, the written operational procedures for inventory control, customs clearance, and accounting operations, together with relevant required documents. Financial institutions may apply to establish a branch office inside the FTZ and conduct foreign exchange business, in accordance with the Banking Law of the ROC, Securities and Exchange Law, Statute Governing Foreign Exchange, and the Central Bank of China Act.

According to Taiwan's Banking Law and Securities Trading Law, in order for a financial institution to conduct foreign currency operations, Taiwan's Central Bank must first grant approval. The financial institution must then submit an application to port authorities to establish an offshore banking unit (OBU) in the free-trade zone. No financial entity has yet applied to establish such an OBU in any of the five free trade zones. An offshore banking unit may operate a related business under the Offshore Banking Act, but cannot conduct any domestic financial, economic, or commercial transaction in New Taiwan Dollars.

Taiwan has promulgated drug-related asset seizure and forfeiture regulations that stipulate that—in accordance with treaties or international agreements—Taiwan's Ministry of Justice shall share seized assets with foreign official agencies, private institutions, or international parties that provide Taiwan with assistance in investigations or enforcement. Assets of drug traffickers, including instruments of crime and intangible property, can be seized along with legitimate businesses used to launder money. The injured parties can be compensated with seized assets. Between January 2007- June 2008, drug-related seizures totaled NT $18,300,000 (approximately $543,150)—a dramatic increase from the NT $1,100,000 (approximately $32,650) the previous year. The Ministry of Justice distributes other seized assets to the prosecutor's office, police or other anti-money laundering agencies. The law does not allow for civil forfeiture. A mutual legal assistance agreement between the American Institute in Taiwan (AIT) and the Taipei Economic and Cultural Representative Office in the United States (TECRO) entered into force in March 2002. It provides a basis for Taiwan and U.S. law enforcement agencies to cooperate in investigations and prosecutions for narcotics trafficking, money laundering (including the financing of terrorism), and other financial crimes.

Although Taiwan is not a UN member and, therefore, cannot be a party to the 1988 UN Drug Convention, the authorities in Taiwan have passed and implemented laws in compliance with the goals and objectives of the Convention. Similarly, Taiwan cannot be a party to the UN International Convention for the Suppression of the Financing of Terrorism, but it has agreed unilaterally to abide by its provisions. Taiwan is a founding member of the Asia/Pacific Group on Money Laundering (APG). The MLPC is a member of the Egmont Group of financial intelligence units.

Taiwan continues to improve and implement an anti-money laundering regime that largely comports with international standards. Taiwan should pass legislation currently before the Legislative Yuan to criminalize terrorism and terrorist financing as an autonomous crime. It should exert more authority over its nonprofit organizations. The MLCA amendments of 2003, 2007, and 2008 address a number of vulnerabilities, especially in the area of asset forfeiture. The authorities on Taiwan should continue to strengthen the existing anti-money laundering regime as they implement the new measures. Taiwan should abolish all shell companies and prohibit new shell companies of any type from being established. Taiwan should enhance implementation of legislation regarding alternate remittance systems and Taiwan law enforcement should enhance investigations of underground finance and its links to trade fraud and trade-based money laundering.

Tanzania

While not an important regional financial center, Tanzania is vulnerable to money laundering. Tanzania's location at the crossroads of southern, central and eastern Africa leave it particularly vulnerable to activities that generate illicit revenue, such as smuggling, and the trafficking of narcotics, arms, and humans. The likely sources of illicit funds are Asia and the Middle East and, to a lesser extent, Europe. Such transactions rarely include significant amounts of U.S. currency. Money laundering is more likely to occur in the informal financial sector and in nonfinancial sectors than in the undeveloped formal sector. Real estate and used car businesses appear to be vulnerable trade industries involved in money laundering. Criminals use front companies, including hawaladars and bureaux de change, to launder funds. The use of front companies to launder money is especially common on the island of Zanzibar, where few federal regulations apply. Officials indicate that money laundering schemes in Zanzibar generally take the form of foreign investment in the tourist industry and bulk cash smuggling.

There are no indications that Tanzania's two free trade zones are being used in trade-based money laundering schemes or by financiers of terrorism. The Anti-Money Laundering Act, 2006 (AML Act) criminalizes cross-border cash smuggling.

The AML Act created a financial intelligence unit (FIU) as an extra-ministerial department of the Ministry of Finance. The government published implementing regulations in September 2007. The AML Act empowers the FIU to receive and share information with foreign FIUs and other comparable bodies. At present, the FIU has a small core staff comprised of a Commissioner, an analyst, an information technology expert, and two support staff. Current plans call for the recruitment of three additional staff members. The FIU has established an office, but has not begun analyzing suspicious transactions. It has applied for membership in the Egmont Group.

The AML Act and regulations apply to all "reporting persons", which includes banks and financial institutions, cash dealers, accountants, real estate agents, dealers in precious stones, customs officers, auctioneers, and legal professionals handling real estate or funds. Reporting persons must obtain detailed information from all customers, maintain specific identification procedures, and report suspicious and unusual transactions to the FIU within 24 hours of the transaction. The AML Act governs all serious crimes, including those relating to both narcotics and terrorism. The FIU has developed a sensitization and outreach program to ensure that obliged institutions are aware of their reporting requirements under the AML Act. The FIU held two sensitization workshops targeting Tanzania's insurance and banking communities in July 2008.

The 2002 Prevention of Terrorism Act criminalizes terrorist financing. It requires all financial institutions to inform the government each quarter of a calendar year of any assets or transactions that may be associated with a terrorist group. However, the implementing regulations for this provision have not yet been drafted. Under the Act, the government may seize assets associated with terrorist groups. The Bank of Tanzania circulates to Tanzanian financial institutions the names of suspected

terrorists and terrorist organizations on the United Nations Security Council Resolution (UNSCR) 1267 Sanction Committee's consolidated list, but by the end of 2008, no assets had been frozen under this provision. It is not clear whether Tanzania has the investigative capacity to identify and seize related assets.

Tanzania has cooperated with the U.S. in investigating and combating terrorism. There are no specific laws allowing Tanzania to exchange records with the U.S. on narcotics transactions or narcotics-related money laundering.

Tanzania is a member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), a Financial Action Task Force-style regional body, and the Secretariat is located in Dar-Es-Salaam. ESAAMLG conducted a mutual evaluation of Tanzania in November 2008, which is scheduled for discussion and adoption in 2009. Tanzania is a party to the 1988 UN Drug Convention; the UN Convention for the Suppression of the Financing of Terrorism; the UN Convention Against Corruption; and the UN Convention against Transnational Organized Crime. In 2008, Tanzania was listed as 102 of 180 countries in Transparency International's Corruption Perceptions Index.

The Government of Tanzania (GOT) has made improvements in its compliance with international AML standards. The GOT should focus its efforts on practical implementation of the AML Act, including dedicating the resources necessary to build an effective FIU. The FIU should continue its efforts to hire additional staff to ensure that financial institutions are adequately supervised, to inform them of their reporting and record-keeping responsibilities, and to train the financial sector to identify suspicious transactions. Authorities should ensure that the Prevention of Terrorism Act comports with international standards and that that the GOT implements all provisions in the law. The GOT should also improve its cross-border cash declaration regime. Tanzania should examine vulnerabilities that it has not yet addressed, in particular the inherent vulnerabilities of alternative remittance systems and trade, and any additional weaknesses posed by less-regulated Zanzibar.

Thailand

Thailand is a centrally located, developed Southeast Asian country surrounded by economically less vibrant neighbors along an extremely porous border. Thailand is vulnerable to money laundering from its own underground economy as well as many categories of cross-border crime, including illicit narcotics and other contraband smuggling. The Thai black market includes a wide range of pirated and smuggled goods, from counterfeit medicines to luxury automobiles. Money launderers and traffickers use banks, as well as nonbank financial institutions and businesses to move the profits of narcotics trafficking and other criminal enterprises. The amount of opium and heroin produced in the Golden Triangle region of Burma, Laos and Thailand has decreased over the past decade as enforcement has escalated and drug traffickers have shifted to importing and distributing methamphetamine tablets as the main drug of choice for domestic Thai consumption. Thailand is a significant destination and source country for international migrant smuggling and trafficking in persons, a production and distribution center for counterfeit consumer goods and, increasingly, a center for the production and sale of fraudulent travel documents. Illegal gambling, underground lotteries, and prostitution are all problems. Underground finance and remittance systems are used to launder illicit proceeds.

Thailand's anti-money laundering legislation, the 1999 Anti-Money Laundering Act (AMLA) and subsequent amendments, criminalize money laundering for the following nine offenses: narcotics trafficking, trafficking in women or children for sexual purposes, fraud, financial institution fraud, public corruption, customs evasion and extortion, public fraud and blackmail, terrorist activity, and illegal gambling. It also criminalizes organizing, without prior permission, otherwise licit gambling activities that include more than 100 players, or involve money in excess of bt10 million (approximately $287,000). In 2003, a Royal Thai Government (RTG) decree under constitutional

authority established terrorism as a criminal offense, and in April 2004, the parliament endorsed that decree as a legal act.

Despite the inclusion of a new predicate offense, the current list of predicate offenses in the AMLA does not meet international best practices standards consistent with the first and second recommendations of the Financial Action Task Force (FATF) 40 Recommendations, which apply the crime of money laundering to all serious offenses or with the minimum list of acceptable designated categories of offenses. Additionally, the definition of "property involved in an offense" in the AMLA is limited to proceeds of predicate offenses and does not extend to instrumentalities of a predicate offense or a money laundering offense.

In November 2007, the National Legislative Assembly (NLA) of the then military government (October 2006—January 2008) approved an amendment that gave law enforcement officers power to tackle seven additional offenses by freezing assets of organizations or individuals suspected of gaining from abuse of natural resources, foreign exchange, share sales, gambling, arms sales, fraudulent bidding on state projects and excise tax fraud. Although a positive step, the list remains deficient under international standards as it excludes, among other crimes, migrant smuggling, counterfeiting, and intellectual property rights offenses.

The AMLA also created the Anti-Money Laundering Office (AMLO), which among other functions serves as Thailand's financial intelligence unit (FIU). AMLO became fully operational in 2001. When first established, AMLO reported directly to the Prime Minister. In October 2002, pursuant to a reorganization of the executive branch and following criticisms that AMLO had been politicized, AMLO was designated as an independent agency under the Minister of Justice. As mandated by the AMLA, AMLO analyzes reports of suspicious and large transactions and is responsible for investigating money laundering cases for civil forfeiture, as well as for the custody and disposal of seized and forfeited property. In addition, AMLO is also tasked with providing training to the public and private sectors concerning the AMLA. AMLO has received 47,216 suspicious transaction reports and has disseminated 148 reports within AMLO and to other agencies.

Under the amendments to the AMLA promulgated in February 2008, an anti-money laundering fund was created to help implement supporting activities and enhance cooperation with other domestic and international jurisdictions. The AMLA also established the Anti-Money Laundering Board, comprised of ministerial-level officials and agency heads. This body serves as a periodic advisory board meeting to set national policy on money laundering issues, to propose relevant ministerial regulations, and to monitor and evaluate enforcement of the AMLA. The law also created the transaction committee, to which the AML board appoints individuals from the following independent entities: the judiciary, the court of justice, the auditor general, the national human rights committee, and the attorney committee. A chairman of the committee is elected among the designated committee members while the Secretary General of AMLO serves as the committee secretary. The committee operates within AMLO to review and approve disclosure requests to financial institutions and government related agencies, as well as asset restraint and seizure requests. Under the amended AMLA, the committee has the power to arrest individuals who commit a predicate offense in order to record his/her statement as preliminary evidence before transferring the person to a police investigator. This must be done within 24 hours. The amended AMLA also gives the committee authority to watchdog the independence and neutrality of the AMLO.

AMLO, the Bank of Thailand (BOT), the Securities and Exchange Commission and the Department of Special Investigation are responsible for investigating financial crimes. During 2007, AMLO prosecuted 83 civil asset forfeiture cases and seized financial assets in the amount of Bt 134.4 million (approximately $3.9 million). The Ministry of Justice houses the Department of Special Investigations (DSI), a criminal Investigative agency separate from the Royal Thai Police (RTP). DSI has responsibility for investigating money laundering (as distinct from civil asset forfeiture actions carried

out by AMLO), and for many of the money laundering predicates defined by the AMLA, including terrorism. The DSI, AMLO, and the RTP all have authority to identify, freeze, and/or forfeit terrorist finance related assets. However, the RTP's skills with regard to white-collar crime of all descriptions remains very low, while DSI has yet to measure up to its mandate and remains in need of considerable capacity building.

AMLO shares information with other Thai law enforcement agencies. For example, it has a memorandum of understanding with Royal Thai Customs which requires the agency to share information and evidence of smuggling and customs evasion involving goods or cash that exceed Bt 1 million (approximately $29,000).

The AMLA requires customer identification, record keeping, and the reporting of large and suspicious transactions, as well as providing for the civil forfeiture of property involved in a money laundering offenses. Under the requirement, financial institutions are required to keep customer identification and specific transaction records for a period of five years from the date an account was closed, or from the date a final transaction occurred, whichever is longer. Individuals and institutions cooperating with law enforcement entities can be protected from liability. In October 2008, the cabinet proposed to the parliament that the range of businesses which have to follow the reporting/identification requirements be broadened to include jewelry and gold shops, automobiles, rental/purchase of businesses or car dealers, real-estate agents/brokers, and antiques shops. In August 2008, the Bank of Thailand re-issued notification to financial institutions (Thai and foreign commercial banks, finance companies and asset management companies) to adopt "know your customer" (KYC) and customer due diligence (CDD) procedures in order to be in line with international best practices under the FATF recommendations on anti-money laundering and combating the financing of terrorism (AML/CTF). While there is no immediate penalty for noncompliance, the Thai central bank takes note of those institutions that do not comply when making decisions regarding them.

Thailand does not have stand-alone secrecy laws. However, the new Consolidated Financial Act in 2008 has a provision providing for bank secrecy to prevent disclosure of client financial information. The new act includes some exceptions, including investigation by a financial regulator and any memorandum for understanding committed with other domestic and overseas regulatory agencies on financial institutions or financial transaction. Therefore, financial institutions must disclose their client and ownership information to AMLO upon demand.

The Bank of Thailand, Securities and Exchange Commission (SEC), and AMLO are empowered to supervise and examine financial Institutions for compliance with anti-money laundering/counterterrorist financial laws and regulations. In an effort to eliminate impediments on the power to examine the financial transactions of private individuals, the BOT has amended existing financial laws by introducing the new Financial Institutions Business Act (FIBA) which combines two financial Institution acts (the commercial banking act B.E. 2505 (ad 1962) and The Act on the Undertaking of Finance Business, Securities Business and Credit Fancier Business, B.E. 2522 (ad 1979). The new FIBA became effective on August 3, 2008. The BOT has been working closely with AMLO to train officers in conducting compliance audits. Further, AMLO intends to establish on-site and off-site audit teams with assistance from the BOT. The main purpose is to provide consultation to institutions that face difficulty in complying with Thai legislation and regulation. No penalties are imposed even when mistaken practices are discovered. Such visits are also intended to help financial institutions become accustomed to the operation of these joint responsibilities of both the AMLO and the BOT.

Anti-money laundering controls are also enforced by other Royal Thai government regulatory agencies; including the Office of the Insurance Commission, an independent body under the Ministry of Finance which was created in 2007 from the old Department of Insurance under the Ministry of Commerce. Financial institutions that are required to report suspicious activities are broadly defined

by the new AMLA as any business or juristic person undertaking banking or nonbanking business, including finance and mortgage finance ("credit financier") businesses, securities firms, insurance businesses, saving cooperative companies, and asset management companies. Land registration offices are also required to report any transaction involving property of bt5 million (approximately $143,000) or greater, or a cash payment of bt2 million (approximately $57,000) or greater, for the purchase of real property but only when a financial institution is not involved in the transaction.

The exchange control act of B.E. 2485 (1942), amended in 1984, states that unlimited amounts of foreign currencies may be brought into Thailand. However, the Ministry of Finance issued a regulation effective October 28, 2007 which requires any person who brings foreign currencies in excess of the equivalent of $20,000 into or out of the country to make a declaration with Thai customs, which in turn reports to the Ministry of Finance. In July 2008, the Bank of Thailand notified all financial Institutions of their reporting obligations under the new regulation

Over the course of 2007 and 2008 the Ministry of Finance and the Bank of Thailand agreed in general to relax regulations on capital movement in order to increase flexibility for Thai businesses in managing their foreign currency needs. Pursuant to that goal any person who obtains foreign currency through the exchange of Thai baht, or by borrowing from financial institutions, can now deposit such currency in Thai financial institutions in amounts up to $1 million for individuals and $100 million for juristic persons. The new regulation also increases the limit for remittances in foreign currencies, up to $1 million per year by Thai residents to overseas destinations (the limit can be up to $5 million per year for purchasing property overseas). There is no restriction on the amount of Thai currency (baht) that may be brought into the country. A person traveling to Thailand's bordering countries, including Vietnam, is allowed to take Thai baht with them up to bt500,000 (approximately $14,300). To all other countries they may take up to bt50,000 (approximately $1,430) without authorization.

Thailand is not an offshore financial center nor does it host offshore banks, shell companies, or trusts. Licenses were first granted to Thai and foreign financial institutions to establish Bangkok International Banking Facilities (BIBFs) in March 1993. However after the United Nations Drug Control Program and the World Bank listed BIBFs as potentially vulnerable to money laundering activities, the Thai government called in BIBF licenses during 2006, citing the BOT's "one presence" policy requiring all financial institutions to upgrade their status to full banks, branches, or subsidiaries, or else exit the market. In October 2006 the last BIBF license was returned to the Bank of Thailand and currently none are operating in the country.

The stock exchange of Thailand requires securities dealers to have "know your customer" procedures, although the set does not check anti-money laundering compliance during its reviews. The Office of Insurance Commission is responsible for the supervision of insurance companies, which are covered under the AMLA definition of a financial institution, but there are no anti-money laundering regulations for the insurance industry. Similarly, the Cooperative Promotion Department (CPD) is responsible for the supervision of credit cooperatives, which are required under the cooperatives act to register with the CPD. Currently 6,117 cooperatives are registered with 1,263 thrift and credit cooperatives engaged in financial business. Thrift and credit cooperatives receive deposits and provide loans to members and come under the definition of a financial institution. As with the securities and insurance sectors, no anti-money laundering compliance mechanisms are in place. Thai authorities have recognized these issues and the expressed the need to address them.

Financial institutions (such as banks, finance companies, savings cooperatives, etc.), land registration offices, and investment advisors or persons who act as solicitors for investors are required to report significant cash, property, and suspicious transactions. Reporting requirements for most financial transaction (including purchases of securities and insurance) exceeding bt2 million (approximately $57,000), and property transactions exceeding bt5 million (approximately $143,600), have been in place since October 2000.

Thailand acknowledges the existence of alternative remittance systems that circumvent financial institutions. There is a general provision in the AMLA that makes it a crime to transfer or receive a transfer from the proceeds of specified criminal offenses, including terrorism. Remittance and money transfer agents, including informal remittance businesses, require a license from the Ministry of Finance, which must be renewed annually. Guidelines issued by the Ministry of Finance and the BOT in 2004 provide for onsite inspections of money changers and money transfer agents by the BOT before licenses may be granted. The BOT also consults with AMLO on the applicant's possible criminal history and AML record. Both moneychangers and remittance agents are required to report suspicious financial transactions to AMLO. Licensed agents are subject to monthly transaction reporting on every transaction and are subject to a five year record maintenance requirements well as to onsite inspections. There are approximately 558 authorized moneychangers and 1,202 remittance agents in Thailand.

Money changers frequently act as illegal remittance agents. In 2004 the Bank of Thailand limited the amount money changers may sell to an individual customer at a maximum of $5,000. Customers must present a passport or other travel document as identification. There is no limit on buying foreign currencies, nor is there an overall annual transaction volume or amount limit. For remittance agents, the BOT limits the daily maximum amount of foreign currency that may be sold to an individual customer to the equivalent of $2,000, and requires a customer to present supporting documents indicating the reason for the transfer. There is no limit on receiving foreign currencies from persons overseas or on payment in baht to recipients In Thailand.

Money and property derived from commission of a predicate offense, from aiding or abetting the commission of a predicate offense, or derived from the sale, distribution, transfer, or returns of such money or assets may be seized under section 3 of the AMLA. AMLO, through the transaction committee, is responsible for tracing, freezing, and seizing assets. The AMLA makes no provision for substitute seizures if authorities cannot prove a relationship between the asset and the predicate offense. Overall, the banking community cooperates with AMLO's efforts to trace funds and seize or freeze bank accounts. BOT does not have regulations that give it explicit authorization to control charitable donations, but works with AMLO to monitor these transactions under the Exchange Control Act of 1942.

In October 2007 the Thai prime minister endorsed a cabinet decision to abolish an incentive system that had gone into effect three years earlier under the "Office of Prime Minister's Regulation on Payment of Incentives and Rewards in Proceedings against Assets under the Anti-Money Laundering Act." Under this now-defunct rewards system, AMLO investigators and their supervisors, as well as other investigative agencies, were eligible to receive personal commissions on the property that they seized. The United States and other countries and international organizations including UNODC, criticized this system on the grounds that it threatened the integrity of its AML regime and created a conflict of interest by giving law enforcement officers a direct financial stake in the outcome of forfeiture cases. The United States additionally halted training and other assistance to AMLO while the rewards practice remained in place. The 2007 order contains a controversial grandfather clause which allows reward payments to continue in cases already approved before the effective termination date of the system.

Thailand is a party to the 1988 UN Drug Convention and the UN Convention for the Suppression of the Financing of Terrorism. It has signed, but not ratified the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. The Royal Thai Government (RTG) has issued instructions to all authorities to comply with UNSCR 1267; including freezing funds or financial resources belonging to suspected terrorists and terrorist organizations listed by UN 1267 Sanctions Committee. To date, Thailand has not identified, frozen, or seized any assets linked to individuals or entities included on the UNSCR 1267 Sanctions Committees' consolidated list. However, AMLO has identified suspicious transaction reports derived from financial institutions and

has initiated cases that they believed may have involved terrorist activities using nongovernmental or nonprofit organizations as a front.

Thailand has mutual legal assistance treaties (MLATS) with 10 countries, including the United States, and is party to the regional ASEAN Mutual Legal Assistance Agreement. AMLO has Memoranda of Understanding (MOU) on money laundering cooperation with 35 other financial intelligence units. It also actively exchanges information with nations with which it has not entered into an MOU, including the United States, Singapore, and Canada. In 2008, AMLO responded to 62 requests for information from foreign FIUs. Thailand cooperates with United States and other nation's law enforcement authorities on a range of money laundering and illicit narcotics related investigations. Thailand is a member of the Asia/Pacific Group on Money Laundering (APG), a FATF-style regional body, and the Egmont Group.

During the past several years, the Royal Thai Government has shown its commitment to the adoption of AML/CTF international best practices. While many improvements have already been identified and adopted by Thai agencies, there are still important pending actions including the passage of key bills, regulations, or measures which will help augment the current AML/CTF regime in Thailand. Nonbank financial institutions and businesses such as gold shops, jewelry stores and car dealers should be subject to suspicious transaction reporting requirement without regard to a monetary threshold. The insurance and securities sectors should institute AML compliance programs. Besides onsite consultation, AMLO should also undertake audits of financial institutions to ensure compliance with requirements of AMLA and AMLO regulations. Until the RTG provides a viable mechanism for all of its financial institutions to be examined for compliance with the AMLA, Thailand's anti-money laundering regime will not fully comport with international standards. In addition, the RTG should develop and implement anti-money laundering regulations for exchange businesses and should take additional measures to address the vulnerabilities presented by alternative remittance systems. The Royal Thai Government should become a party to the UN convention against Transnational Organized and to the UN Convention against Corruption.

Trinidad and Tobago

Trinidad and Tobago (T&T) has a well-developed and modern banking sector that makes it an increasingly significant regional financial center. Currently, the country does not offer offshore banking, and the government is working to launch an international financial center. Drug-trafficking, illegal arms sales and fraud continue to be the most prevalent sources of laundered funds. The authorities consider illicit drug-trafficking to be the primary predicate offense with regard to money laundering. Criminal assets laundered in T&T are primarily derived from domestic criminal activity as well as from the activity of nationals involved in crime abroad. While there is no significant black market for smuggled goods in T&T, drug money continues to support the importation of illegal arms at a rate that is suspected to be growing. According to information from financial institutions and legal analysts, financial crimes in general are increasing, particularly those involving the use of fraudulent checks, wire transfers, and related instruments in the banking sector. T&T's financial institutions are not known to engage in currency transactions involving international drug-trafficking proceeds that significantly affect the United States. There is no indication the government itself or government officials encourage, facilitate or engage in money laundering.

Despite the increasing number of crimes and the desire to become an international financial center, the Government of Trinidad & Tobago (GOTT) has made no significant improvement to its anti-money laundering (AML) regime since late 2005, when a mutual evaluation conducted by the Caribbean Financial Action Task Force (CFATF), a Financial Action Task Force (FATF)-style regional body, found T&T noncompliant with most FATF Recommendations and in full compliance with only one.

There are six free trade zones (FTZs) in Trinidad and Tobago where exporting of services and manufactured products, and re-exportation of manufactured products take place. There is no evidence the FTZs are involved in money laundering schemes, and companies operating in the FTZs are required to submit tax returns quarterly and audited financial statements yearly. Companies must present proof of legitimacy and are subject to background checks prior to being allowed to operate in the FTZs.

The Proceeds of Crime Act of 2000 (POCA) defines money laundering and related crimes as serious offenses. The POCA requires financial institutions to actively report suspicious transactions and to maintain records necessary to reconstruct transactions for a number of years. Secrecy laws are limited to standard client confidentiality provisions. There are no measures for sharing of information between financial institutions due to a lack of legislation. Any existing requirements promoting correspondent banking are only applicable to those financial institutions supervised by the Central Bank of Trinidad & Tobago (CBTT). Under the POCA, any officer who aids and abets the money laundering activities of an institution can be convicted of money laundering. Additionally, the POCA protects individuals who cooperate in money laundering law enforcement investigations. The POCA also enables the courts to seize the proceeds of all serious crimes. However, for money laundering offenses, the POCA only recognizes property as being the proceeds of crime when a person has been convicted of a predicate offense. To date, only one property has been seized under the Act.

The CBTT has set AML guidelines, including due diligence provisions that apply to all financial institutions subject to the 1993 Financial Institutions Act. These include banks, finance companies, leasing corporations, merchant banks, mortgage institutions, unit trusts, financial services businesses and financial intermediaries. Credit unions are not subject to the CBTT's regulation; legislation to correct this flaw has been under consideration for several years. In 2004, the CBTT updated its guidelines, setting new minimum standards for compliance with existing regulations that incorporate the basic tenets of the FATF Forty Recommendations and the Nine Special Recommendations. However, continuing deficiencies preclude satisfactory customer due diligence in practice.

There is no indication the GOTT has adopted a risk-based approach to combating money laundering and terrorist financing at the national level. According to the CFATF, no risk assessment has been done to identify and measure vulnerability in the country. The CBTT does use a risk assessment approach with regard to its supervisory functions in evaluating individual institutions. It also has advised its supervised institutions to implement risk-based systems with regard to money laundering issues.

GOTT customs regulations require that currency or monetary instruments totaling more than approximately $10,000 be declared upon entering or leaving the country. GOTT Customs may restrain cash for 96 hours, longer with judicial approval, pending the determination of their source. The Financial Investigations Unit (FIU), housed in the Ministry of National Security, maintains a database of these transactions and analyzes them for evidence of money laundering.

For the period of January—September 2008, GOTT officials reported 417 financial investigations stemming from 13,632 suspicious activity reports. The GOTT received 20 foreign intelligence requests and 101 requests from local institutions. Full year data is not available. Enforcement of suspicious activity reporting remains weak. Most designated institutions have never submitted a report to the authorities, either through lack of suspicious activity or lack of awareness of the requirement. In 2004, the GOTT established a Tax Fraud Investigations unit within its Inland Revenue Division to address tax evasion and nonreported or underreported income that may be derived from money laundering activities.

A 2004 investigation of fraud indicated that during the bidding for and construction of the new Piarco airport, a number of individuals may have committed wire fraud and bank fraud from 1996 to 2001. As a result, in August 2006, two Trinidadian businessmen, other businessmen and two Trinidadian

companies were indicted by a U.S. grand jury for a money laundering conspiracy. At year end 2008, the courts continue to hear this case and related corruption charges against others.

The GOTT has a number of pieces of legislation in place that allows it to trace, freeze, and seize assets, including intangible assets such as bank accounts. Authorities also may seize legitimate businesses if they are used to launder drug money. However, the GOTT can only restrain assets through due process at the level of the High Court—it cannot freeze assets "without undue delay," or on a police investigation warrant. The law only allows for forfeiture of assets in criminal cases, not in civil cases. The GOTT does not have legislation that specifically authorizes the sharing of forfeited assets with other countries, but has done so in the past on a case-by-case basis through bilateral agreements. In 2008, no assets were restrained or confiscated by the High Courts.

Legal loopholes exist that allow traffickers and supporters or financiers of terrorists or terrorist organizations to shield their assets. These include the absence of regulations to prohibit the establishment of shell banks, the ability of attorneys to operate accounts in their clients' names, the absence of suspicious transaction reporting requirements for attorneys and accountants, and legal rules that prevent courts from confiscating assets received after a defendant's sentencing.

The GOTT enacted its Anti-Terrorism Act in September 2005. The GOTT is developing regulations to implement this act, specifically with regard to monitoring financial activities, including alternative remittance systems or donations to suspect organizations. The GOTT has circulated to its financial institutions the names of individuals and entities linked to Usama Bin Laden, al-Qaida, or the Taliban included on the UN 1267 Sanctions Committee's consolidated list. The GOTT has also circulated the United States' list of Specially Designated Global Terrorists and other similar EU lists. There has not yet been any identified evidence of terrorist financing in T&T.

In 1999, a Mutual Legal Assistance Treaty (MLAT) with the United States entered into force, and in 2000, the United States and GOTT signed a joint statement on law enforcement cooperation. This statement pledges, in part, to expand cooperation on the detection and prosecution of money laundering and related criminal activities. While there is no institutionalized procedure in place with the USG for the exchange of crime and terrorism-related information, the GOTT has cooperated regularly with the USG and other governments' law enforcement agencies on issues involving illegal drug-trafficking, terrorism, terrorist financing and other crime investigations.

Trinidad and Tobago is a party to the 1988 UN Drug Convention, the UN Convention against Corruption, and the UN Convention against Transnational Organized Crime. It has not yet signed the UN Convention for the Suppression of the Financing of Terrorism, although this convention is referenced in the Anti-Terrorism Act. Trinidad and Tobago is a member of the CFATF, which is headquartered in Port of Spain. Trinidad and Tobago is also a member of the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD).

The major concern in Trinidad and Tobago is a lack of comprehensive anti-money laundering/counterterrorist financing (AML/CTF) legislation, including necessary enforcement regulations. The existing laws are not in accordance with international standards and are ineffective in that there have been no AML convictions in six years. Currently, there are three proposed pieces of legislation, the POCA Amendment, the FIU Act, and the Financial Obligations Regulations, that should address many of the FATF Recommendations. Nevertheless, due to T&T's legislation process, no significant advance in passing and implementing these laws was realized in 2008. T&T should enact the pending legislation and amend existing legislation, as necessary to bring it in line with international standards. In addition, the Government of Trinidad and Tobago should take steps to address the insufficiency of customer due diligence practices. The GOTT should ensure a comprehensive AML/CTF framework compliant with FATF Recommendations is in place before

launching its proposed international financial center. Trinidad and Tobago should move expeditiously to become a party to the UN Convention for the Suppression of the Financing of Terrorism

Turkey

Turkey is an important regional financial center, particularly for Central Asia and the Caucasus, as well as for the Middle East and Eastern Europe. It continues to be a major transit route for Southwest Asian opiates moving to Europe. However, narcotics-trafficking is only one source of the total funds laundered in Turkey. Other significant sources of laundered funds include invoice fraud and tax evasion, and to a lesser extent, smuggling, counterfeit goods, forgery, robbery, and kidnapping. Terrorist financing and terrorist organizations with suspected involvement in narcotics-trafficking and other illicit activities are also present in Turkey. Money laundering takes place in banks, nonbank financial institutions, and the underground economy. Informed observers estimate as much as 40 to 50 percent of the economic activity is derived from unregistered businesses. Money laundering methods in Turkey include: the large-scale cross-border smuggling of currency; bank transfers into and out of the country; trade fraud; and the purchase of high-value items such as real estate, gold, and luxury automobiles. Turkish-based traffickers transfer money and sometimes gold via couriers, the underground banking system, and bank transfers to pay narcotics suppliers in Pakistan or Afghanistan. Funds are often transferred to accounts in the United Arab Emirates, Pakistan, and other Middle Eastern countries.

In 2005, the Government of Turkey (GOT) passed a tax administration reform law, with the goal of improving tax collection. The GOT is working on additional reforms to combat the unregistered economy and move these businesses onto the tax rolls. In October 2008, as a measure against the global liquidity crunch, the Government submitted a draft bill to the Parliament seeking to encourage the transfer back to Turkey of funds held in off-shore accounts as of October 1, 2008. There has been some concern that this legislation will result in the relaxation of some anti money laundering and counterterrorist financing (AML/CTF) measures, however, GOT officials say this proposal will provide a one-time amnesty for a limited period only for tax evasion and export invoice fraud, but no other offenses.

Alternative remittance systems are illegal in Turkey, and only banks and authorized money transfer companies are permitted to transfer funds. Trade-based money laundering, fraud, and underground value transfer systems also are used to avoid taxes and government scrutiny. There are 21 free trade zones operating in Turkey. The GOT closely controls access to the free trade zones. Turkey is not an offshore financial center.

Turkey first criminalizes money laundering through the Law on Prevention of Money Laundering (Law 4208 of November 19, 1996). Under the law, whoever commits a money laundering offense faces a sentence of two to five years in prison, and is subject to a fine of double the amount of the money laundered, plus asset forfeiture provisions. The Council of Ministers subsequently passed a set of regulations that require the filing of suspicious transaction reports (STRs), know-your-customer (KYC) provisions, and bank maintenance of transaction records for five years.

Prior to the enactment of a new Criminal Code (Law 5237 of June 1, 2005), Turkey's anti-money laundering (AML) law contained a list of specific predicate offenses. The present code defines money laundering predicate offenses as all offenses for which the punishment is imprisonment for one year or more. In 2006, the GOT enacted additional anti-money laundering legislation, the Prevention of Laundering Proceeds of Crime Law of October 18, 2006 (Law 5549), a new criminal law, and a new criminal procedures law.

Under a 2007 Ministry of Finance (MOF) banking regulation circular, all banks and regulated financial institutions, including the Central Bank, securities companies, post office banks, and Islamic

financial houses are required to record tax identity information for all customers opening new accounts, applying for checking accounts, or cashing checks. The circular also requires exchange offices to sign contracts with their clients. The MOF also mandates that a tax identity number be used in all financial transactions. The requirements are intended to increase the GOT's ability to track suspicious financial transactions. According to Article 5 of the anti-money laundering law, public institutions, individuals, and corporate bodies must submit information and documents as well as adequate supporting information upon the request of Turkey's Financial Crimes Investigation Board (MASAK) or other authorities specified in Article 3 of the law. Individuals and corporate bodies from whom information and documents are requested may not withhold the requested items by claiming privacy protection. Despite the increase in information collected for new accounts and transactions, customer due diligence (CDD) and other preventive measures have not yet been fully implemented, and Turkey has not adopted a risk-based regulatory approach. There are no requirements for ongoing CDD and only limited requirements for the collection of beneficial ownership information. There is no requirement for financial institutions to exercise enhanced due diligence on business relationships or transactions with suspicious persons, including persons from or in countries which do not sufficiently apply the FATF recommendations

A new Banking Law was enacted in 2005 to strengthen bank supervision. The Banking Regulatory and Supervisory Agency (BRSA) conducts periodic anti-money laundering and compliance reviews under the authority delegated by MASAK.

Turkey does not have foreign exchange restrictions. With limited exceptions, banks and special finance institutions must inform authorities within 30 days about transfers abroad exceeding $50,000 (approximately 77,500 new Turkish liras) or its equivalent in foreign currency notes (including transfers from foreign exchange deposits). Travelers may take up to $5,000 (approximately 7,750 new Turkish liras) or its equivalent in foreign currency notes out of the country. Turkey does have cross-border currency reporting requirements, and the law gives Customs officials the authority to sequester valuables of travelers who make false or misleading declarations and impose fines for such declarations.

MASAK was established as part of the MOF by the 1996 AML law and became operational in 1997. As Turkey's Financial Intelligence Unit (FIU), MASAK receives, analyzes, and refers STRs for investigation. MASAK has three functions: regulatory, financial intelligence, and investigative. MASAK plays a pivotal role between the financial and law enforcement communities.

The laws explicitly provide safe harbor protection to the filers of STRs. The laws also cover a range of entities subject to reporting requirements, to include several designated nonfinancial businesses and professions (DNFBPs), such as art dealers, insurance companies, lotteries, vehicle sales outlets, antique dealers, pension funds, exchange houses, jewelry stores, notaries, sports clubs, and real estate companies. While the legislation has been improved to require reporting from a wide range of industries and entities, most STRs continue to be submitted by banks.

The number of STRs filed has been relatively low, even taking into consideration the fact that many commercial transactions are conducted in cash. In 2007, 2,946 STRs were filed, of which 144 were linked to terrorist financing activities. Submissions in 2007 were more than double the 1,140 filed in 2006. The safe harbor provision is one reason for this increase. In 2005 and 2004, the levels of STR filings were 352 and 288, respectively. Despite the increase in filings of STRs, these numbers still represent a very low level of overall reporting, given the relatively large size and high level of development of the Turkish financial sector. STR reporting by nonbank entities is increasing but is still a small fraction of STRs. In 2007, there were 40 STRs from brokerage houses and three STRs from insurance companies.

With the passage of several new pieces of legislation, the Government of Turkey took steps in 2006 and 2007 to strengthen its AML/CTF regime. The GOT now faces the challenge of aggressively

implementing these laws. In 2007, the GOT established a High Coordination Council on Financial Crimes, which consists of representatives of MASAK, the MOF, the Capital Markets Board, and the Central Bank. The aim of this council is to improve coordination among the agencies to combat financial crimes and support the work of MASAK. MASAK is working on improving its automation to be able to access banks' and other financial institutions' data bases, in order to accelerate the review process and to enable it to refer cases more quickly to prosecutors.

The law gives MASAK the authority to instruct a number of inspection bodies (such as bank examiners, financial inspectors, or tax inspectors) to initiate an investigation if MASAK has reason to suspect financial crimes. Likewise, MASAK can refer suspicious cases to the public prosecutor and the public prosecutor can ask MASAK to conduct a preliminary investigation prior to referring a case to the police for criminal investigation. In January 2007, a regulation on money laundering crime was enacted enhancing MASAK's authority to combat these crimes. In 2007, MASAK increased its efforts to train specialists in law enforcement units and judicial authorities on money-laundering and terrorist financing, with a goal to increase the number of money laundering and terrorist financing of prosecutions.

According to MASAK statistics, as of December 31, 2007 it had pursued 2,274 money laundering investigations since its 1996 inception. Between 2003 and 2007, there were 1,424 money laundering files, of which 338 were referred for further investigation with evidence of predicate offense, but only ten cases resulted in convictions. Moreover, all of the convictions are reportedly under appeal. There is a lack of specialization and understanding of AML/CTF provisions among relevant authorities, which has contributed to the high number of acquittals in money laundering cases. As of December 31, 2007, 47.4 percent of the cases referred to prosecutors were narcotics related. In 2007, the GOT opened 22 money laundering cases, of which five resulted in a conviction.

Turkey has a system for identifying, tracing, freezing, and seizing assets that are not related to terrorism, although the law allows only for their criminal, but not administrative, forfeiture. Article 7 of the AML law provides for the confiscation of all property and assets (including derived income or returns) that are the proceeds of a money laundering predicate offense (recently expanded to include crimes punishable by one year imprisonment) after conviction. The law allows for the confiscation of the instrumentalities of money laundering and the equivalent value of direct proceeds that could not be seized. In addition to the AML law, Articles 54 and 55 of the Criminal Code provide for post-conviction seizure and confiscation of the proceeds of crimes. The defendant, however, must own the property subject to forfeiture. Legitimate businesses can be seized if used to launder drug money or support terrorist activity, or are related to other criminal proceeds. Property or its value that is confiscated is transferred to the Treasury.

The GOT enforces existing drug-related asset seizure and forfeiture laws. MASAK, prosecutors, Turkish National Police, and the courts are the government entities responsible for tracing, seizing and freezing assets. According to Article 9 of the AML law, the Court of Peace—a minor arbitration court for petty offenses—has the authority to issue an order to freeze funds held in banks and nonbank financial institutions as well as other assets, and to hold the assets in custody during the preliminary investigation. During the trial phase, the presiding court has freezing authority. Public prosecutors may freeze assets in cases where it is necessary to avoid delay. The Public Prosecutor's Office notifies the Court of Peace about the decision within 24 hours. The Court of Peace has 24 hours to decide whether to approve the action. There is no time limit on freezes. There is no specific provision in Turkish law for the sharing of seized assets with other countries; however the United States and Turkey shared seized assets in one narcotics case.

Financing of terrorism is criminalized for the first time in July 2006 by Law 5532, which amends the existing Anti-Terror Law (3713). Law 5549 includes significant provisions to prevent money laundering and terrorist financing. However, deficiencies in the scope and detail of the terrorist

financing offense are noted in the 2007 FATF evaluation. Specifically, the law's coverage currently is limited to acts committed by members of organizations against the Turkish Republic by force and violence using terror, intimidation, oppression or threat. This means the collection, donation and movement of funds by terrorist organizations would not be prohibited if the funds could not be linked to a specific domestic terrorist act. Because the law also does not include a requirement for reporting suspicious transactions related to terrorist financing, the GOT issued a General Communiqué of Suspicious Transaction Reporting Regarding Terrorist Financing, which entered into force in November 2007. Turkey issued additional regulations to combat terrorist financing in January 2008, within the context of the money laundering legislation adopted in 2006. The regulation entered into force in April 2008.

MASAK's General Communiqué No. 3, dated February 2002, requires that a special type of STR be filed by financial institutions in cases of suspected terrorist financing. However, until the amendments to the criminal code were enacted in June 2006, terrorist financing was not explicitly defined as a criminal offense under Turkish law. Various laws exist with provisions that can be used to punish the financing of terrorism. These include Articles 220, 314 and 315 of the Turkish penal code, which prohibit assistance in any form to a criminal organization or to any organization that uses or threatens violence to influence public services; media; proceedings of bids, concessions, and licenses; or to gain votes.

Although the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee consolidated list, as well as U.S.-designated names, are routinely distributed to financial institutions and appropriate Turkish agencies, Turkey has not taken sufficient steps to implement an effective regime to combat terrorist financing, especially as it relates to UNSCRs 1267 and 1373. For example, while the GOT has implemented UNSCR 1267, it has failed to establish punishment or sanctions for institutions that fail to observe a freezing order, and it has not established procedures for delisting entities or unfreezing funds. Additionally, the GOT has not taken steps that would allow it to freeze the assets of entities designated by other jurisdictions, as required under UNSCR 1373.

Another area of vulnerability regarding terrorist financing is the GOT's supervision of nonprofit organizations. The nonprofit sector is well regulated, but it is not audited on a regular basis for CTF vulnerabilities and does not receive adequate AML/CTF outreach and guidance from the GOT. The General Director of Foundations (GDF) issues licenses for charitable foundations and oversees them. However, there are a limited number of auditors to cover more than 70,000 institutions. The Ministry of Interior regulates charitable nongovernmental associations (NGOs). The GDF, as part of the Ministry of Interior, keeps central registries of the charitable organizations it regulates. It also requires charities to verify and prove their funding sources and to have bylaws. Charitable organizations are required to submit periodic financial reports to the regulators. The regulators and the police closely monitor monies received from outside Turkey. The police also monitor NGOs for links to terrorist groups.

In the months after 9/11, the Council of Ministers decreed (2482/2001) all funds and financial assets of individuals and organizations included on the UNSCR 1267 Sanctions Committee's consolidated list be frozen. However, the tools available at that time under Turkish law for locating, freezing, seizing, and confiscating terrorist assets were cumbersome, limited, and ineffective. In late 2001, the Council of Ministers froze the funds of one individual accused of financing terror in Turkey. A series of appeals and conflicting rulings by various courts prolonged the application of these provisions until 2007, but eventually the courts upheld the first application of the freezing authority. The assets of two listed individuals continue to be frozen under the 1267 designations. Changes in law relating to MASAK, the Turkish criminal code, and the anti-terrorism law give more authority to seize and freeze assets quickly and make the Turkish system more compliant with international standards. According to MASAK statistics, no assets linked to terrorist organizations or terrorist activities were frozen in 2007.

The GOT cooperates closely with the United States and with its neighbors in the Southeast Europe Cooperation Initiative (SECI). Turkey and the United States have a Mutual Legal Assistance Treaty (MLAT) and cooperate closely on narcotics and money laundering investigations. Turkey is a member of the FATF. Since 1998, MASAK has been a member of the Egmont Group. Turkey is a party to the 1988 UN Drug Convention, the UN Convention for Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption.

While AML legislation has been strengthened and expanded from what previously existed, many provisions have not been tested, prosecution and convictions remain low, and penalties for money laundering offenses remain insufficient. Moreover, there appears to be an over-reliance on STRs to initiate money laundering investigations. To better investigate and prosecute such cases, law enforcement and judicial authorities should enhance their capacity on AML/CTF issues. Law enforcement and Customs authorities should be able to follow money and value trails during the course of their investigations, and should not be required to turn that portion of the investigation over to MASAK. MASAK should ask for expert help from the Turkish National Police or prosecution offices to fulfill its mandate to investigate promptly preliminary indications of money laundering. The GOT also should regulate and investigate remittance networks to thwart their potential misuse by terrorist organizations or their supporters. The GOT should fully implement the provisions of UNSCRs 1267 and 1373, and should consider expanding its narrow legal definition of terrorism. The GOT must also strengthen its oversight of foundations and charities, which currently receive only cursory overview and auditing. Turkey should take steps to improve the CDD procedures and other preventative measures, as well as adopt a risk-based approach to AML/CTF. The GOT should improve supervision and regulation of DNFBPs covered by the 2006 legislation.

Turks and Caicos

The Turks and Caicos Islands (TCI) is an overseas territory of the United Kingdom (UK) comprised of over 40 different islands and forms the southeastern end of the Bahamas archipelago. The country's geographic location has made it a transshipment point for narcotics traffickers. The TCI is vulnerable to money laundering due to its significant offshore financial services sector, drug trafficking and notable deficiencies in its anti-money laundering and counterterrorist financing regime. Perceptions of public corruption continue. Based upon a recommendation of the UK Overseas Territories Report, TCI established a commission of inquiry in July 2008 to probe public corruption by TCI's past and present members of the House of Assembly. In addition, the UK is sending two administrators to provide direction and management of all government funds in the territory.

The TCI's well developed financial and designated nonfinancial sectors are comprised of approximately eight banks; seven money remitters, one casino, 67 real estate agents, ten jewelers, 35 lawyers, 26 accountants, 41 corporate service providers, 19 professional trustees, and 2,500 insurance companies. As of July 2007, 14,746 "exempt companies" or International Business Companies (IBCs) were of record with the Companies Registry. IBCs are permitted to issue bearer shares. The Companies (Amendment) Ordinance 2001 requires that bearer shares be immobilized by depositing them, along with information on the share owners, with a defined licensed custodian. IBCs are required to keep a register of its members and to file a list of members and the shares held by each member with the Companies Register annually. Trust legislation allows establishment of asset protection trusts insulating assets from civil adjudication by foreign governments; however, the Superintendent of Trustees has investigative powers and may assist overseas regulators. As such, TCI remains something of a "tax haven" for foreign criminals seeking to evade domestic tax reporting requirements.

The Financial Services Commission (FSC) licenses and supervises banks, money transmitters, mutual funds and funds administrators, investment dealers, trust companies, insurance companies and agents,

and company service providers. It also licenses IBCs and acts as the Company Registry for the TCI. The FSC conducts on-site and off-site examinations to determine compliance with TCI laws and regulations and has the ability to issue sanctions for noncompliance. The FSC subscribes to a risk based approach, and regulations and guidelines require financial institutions to adopt a risk based approach to their internal controls and procedures. The Financial Services Commission has a staff of 21, including four regulators. The FSC became a statutory body under the Financial Services Commission Ordinance 2001 and preserved under the Financial Services Commission Ordinance 2007. It reports directly to the Governor, as well as to the Minister of Finance.

The 1998 Proceeds of Crime Ordinance (PCO) criminalizes money laundering related to all crimes and provides "safe harbor" protection for good faith compliance with reporting requirements. The PCO also establishes a Money Laundering Reporting Authority (MLRA) to receive, analyze and disseminate financial disclosures such as suspicious activity reports (SARs). The Proceeds of Crime Ordinance 2007 (POCO) consolidates pre-existing provisions and updates legislation related to money laundering. The POCO criminalizes money laundering; provides for the confiscation of the proceeds of crime; permits civil forfeiture; enhances the powers of the MLRA; requires financial institutions to report suspicious activity to the MLRA; and gives the Supreme Court the power to make a number of orders to assist the police in money laundering investigations.

Chaired by the Attorney General, the MLRA is also comprised of the Collector of Customs, the Managing Director of the FSC and the Head of the Financial Crimes Unit (FCU), the Commissioner of Police, and the Superintendent of the Criminal Investigation Department. The Financial Crimes Unit (FCU) of the Royal Turks and Caicos Islands Police is the designated financial intelligence unit (FIU) of the Turks and Caicos and as such manages the responsibilities of the MLRA. The FCU is comprised of five officers. In addition to receiving, analyzing, and investigating SARs, the FCU is also responsible for investigating large cash seizures, local drug traffickers and other serious financial crimes. For 2007, the FCU received 25 SARs (no statistics were available for 2008). The FCU is authorized to disclose information it receives to domestic law enforcement and foreign governments and does not require a memorandum of understanding (MOU) in order to exchange information. The FCI should have more operational independence, provide more guidance and feedback to financial institutions, and release periodic reports on its statistics.

The POCO, the Anti-Money Laundering Regulations (AMLR) (revisions) 2007 and the Anti-Money Laundering and Prevention of Terrorist Financing Code (the Code) 2007 impose obligations on the regulated financial sector to put in place and implement procedures to prevent money laundering. The AMLR place additional requirements on the financial sector such as identification of customers, mandates retention of records, training of staff on money laundering prevention and detection, and development of internal procedures to ensure proper reporting of suspicious transactions. The POCO and the AMLR also apply and impose obligations on certain other relevant businesses specified in the AMLR including dealers in high value goods, dealers in precious metals and stones, real estate agents, casinos, accountant and lawyers. The Code, as guidance, applies to regulated entities licensed and regulated by the FSC and to designated nonfinancial businesses and professions. The Money Transmitters Services Bill was introduced to Parliament and is expected to be passed in 2009. This legislation will fully bring money transmitters under the TCI's anti-money laundering (AML) and counterterrorist financing (CTF) regime.

The AMLR prohibits regulated financial institutions from having a correspondent relationship with shell banks. The Code covers customer due diligence (CDD) requirements and requires financial institutions to pay attention to unusual and large transactions. However, the requirement to conduct CDD on customers carrying out occasional wire transfers is not covered by the AMLR and the Code. Furthermore, the AMLR does not address enhanced due diligence, as there is no requirement to take additional steps in high risk scenarios such as transactions involving politically exposed persons. The Code stipulates that records must be kept for five years; however, requirements to maintain adequate

records are not clearly specified in enforceable legislation and regulations. Therefore, record retention is essentially done on a voluntary basis. Anonymous accounts are permitted.

The POCO provides for criminal and civil asset forfeiture. The Court and prosecutorial authorities are able to make confiscation and forfeiture orders once a person has been convicted of an indictable offense and proven that they have benefited from criminal conduct. Civil forfeiture does not require an individual to be convicted of an offense. The POCO also provides for production and freeze orders to identify, trace, and restrain assets where a money laundering investigation has been initiated or where money laundering proceedings have begun. However, TCI has no domestic provisions for coordinating restraint and confiscation actions with other countries, and no provisions for sharing of confiscated assets, although it does cooperate informally with other countries in confiscation matters.

Travelers entering or leaving the TCI with more than $10,000 must make a declaration to Customs officials. There is no provision for the restraint of cash by Customs Officers when a false declaration is made. An MOU between Customs and the Police (which includes the FCU) permits the exchange of seizure information.

As a UK territory, the TCI is subject to the United Kingdom Terrorism (United Nations Measure) (Overseas Territories) Order 2001, al-Qaida and Taliban (United Nations Measure) (Overseas Territories) Order 2002, and the Anti-Terrorism (Financial and Other Measures) (Overseas Territories) Order 2002. Financial institutions are required to file quarterly reports indicating whether or not they are in possession of terrorist property. AML/CTF requirements do not apply to charities and nonprofit organizations. To date, the FCU has not received any SARs related to terrorism financing.

The TCI cooperates with foreign governments—in particular, the United States and Canada—on law enforcement issues, including narcotics trafficking and money laundering. The FCU also shares information with other law enforcement and regulatory authorities inside and outside of the TCI. The Overseas Regulatory Authority (Assistance) Ordinance 2001, allows the TCI to further assist foreign regulatory agencies. This assistance includes search and seizure powers and the power to compel the production of documents. However TCI should implement domestic provisions which allow for the enforcement of foreign restraining and confiscation orders, and the sharing of assets confiscated as a result of such cooperation.

The 1988 UN Drug Convention applies to the TCI by extension. The FIU became a member of the Egmont Group in 2008. The Mutual Legal Assistance Treaty between the United States and the United Kingdom concerning the Cayman Islands was extended to the TCI in November 1990. The TCI does not have a Tax Information Exchange Agreement with the United States. The TCI is a member of the Caribbean Financial Action Task Force (CFATF), a FATF-style regional body and underwent a mutual evaluation that was finalized in December 2008. The evaluation noted improvements to the TCI's AML/CTF regime, as well as significant deficiencies including the following: The TCI needs to define and make arrangements to circulate designated terrorist lists to financial institutions and provide guidance to meet necessary obligations in this regard; the Code does not address guidelines for reporting entities in relation to their obligation to freeze terrorist assets; except for trust and company service providers, there is not effective AML/CTF framework in place for designated nonfinancial businesses and professionals; there are no requirements for financial institutions to perform enhanced due diligence for higher risk categories of customer, business relationships or transactions; there are no measures in place to cover domestic, cross-border, and nonroutine wire transfers; the FCU does not produce any reports or provide information regarding their activities or trends and typologies; and the FCU has not provided guidance to financial institutions and other reporting entities regarding the reporting of STRs.

In March 2008, the United Kingdom published The Foreign and Commonwealth Office: Managing Risk in the Overseas Territories. In terms of AML/CTF, the Foreign and Commonwealth Office indicated that regulatory standards in most Territories are not up to those of the Crown Dependencies

of Jersey, Guernsey, and the Isle of Man) and that a lack of capacity has reduced the ability of Territories to investigate and prosecute money laundering. The report particularly noted that capacity limitations in the offshore financial sector have limited Territories' ability to investigate suspicious activity reports, and, in the case of the TCI resources are inadequate to keep up with increasingly sophisticated international standards and products in offshore financial services. The report noted that only the Cayman Islands has, so far achieved successful prosecutions of local participants for offshore money laundering offenses. There has not been any money laundering convictions in TCI since 2002.

The Government of the Turks and Caicos Islands with one of the largest and most developed offshore sectors should correct all the deficiencies noted in the CFATF mutual evaluation to be in full accordance with international standards; extend existing regulations to all sectors, bringing all obligated entities under the supervision of a regulatory body, enhance customer due diligence requirements to close existing loopholes, clearly specifying requirements to maintain adequate records in enforceable legislation and regulations, and bolster its on-site supervision program. The TCI should expand efforts to cooperate with foreign law enforcement and administrative authorities. The FCU should conduct awareness training that includes providing guidance on the procedures for reporting STRs including reporting timeframes. The TCI should work to fully develop its capacity to investigate and prosecute money laundering and terrorist financing cases. And the TCI should provide adequate resources and authorities to provide supervisory oversight of its offshore sector to further ensure criminal or terrorist organizations do not abuse the Turks and Caicos Islands' financial sector.

Ukraine

Corruption, organized crime, prostitution, smuggling, tax evasion, and trafficking in persons, drugs and arms continue to be sources of laundered funds in Ukraine. As of November 1, 2008, Ukraine has 184 licensed banks, two of which are state-owned. There are no offshore financial centers or facilities under Ukraine's jurisdiction.

In January 2001, the Government of Ukraine (GOU) enacted the "Act on Banks and Banking Activities," which introduces some anti-money laundering (AML) requirements for banking institutions. The Act prohibits banks from opening accounts for anonymous persons, requires the reporting of large transactions and suspicious transactions to state authorities, and provides for the lifting of bank secrecy pursuant to an order of a court, prosecutor, or specific state body. In August 2001, the President signed the "Law on Financial Services and State Regulation of the Market of Financial Services." This law establishes regulatory control over nonbank financial institutions that manage insurance, pension accounts, financial loans, or "any other financial services involving savings and money from individuals." The law provides definitions for "financial institutions" and "services," imposes record keeping requirements on obligated entities, and identifies the responsibilities of regulatory agencies. The law establishes the State Commission on Regulation of Financial Services Markets (SCFM), which, along with the National Bank of Ukraine (NBU) and the State Commission on Securities and the Stock Exchange, has responsibility for regulating financial services markets.

The Financial Action Task Force (FATF) placed Ukraine on the list of noncooperating countries and territories (NCCT) in September 2001. Following substantial efforts to adopt appropriate legislation and institute an enforcement regime, FATF removed Ukraine from all monitoring in 2006. The Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), a FATF-style regional body (FSRB), conducted a third-round evaluation of Ukraine in September 2008, with a report due for release in March 2009.

The Criminal Code of Ukraine has separate provisions criminalizing drug-related and nondrug-related money laundering. Amendments to the Code adopted in January 2003 include willful blindness

provisions and expand the scope of predicate crimes for money laundering to include any action punishable under the Criminal Code with imprisonment of three years or more, excluding certain specified actions.

On November 28, 2002, the President signed into law Ukrainian Law No. 249-IV, an AML package entitled "On Prevention and Counteraction of the Legalization (Laundering) of the Proceeds from Crime" (the Basic AML Law). The Basic AML Law establishes a two-tiered system of financial monitoring consisting of initial financial monitoring (i.e., obligated entities that carry out financial transactions) and state financial monitoring (i.e., government agencies charged with regulation and supervision of the financial institutions). Overall regulatory authority is vested in the SCFM, in accordance with Article 4 of the Basic AML law.

To correct deficiencies in the Basic AML Law, legislation enacted in February 2003 requires banks and other financial service providers to implement AML compliance programs, conduct due diligence to identify beneficial account owners prior to opening an account or conducting certain transactions, report suspicious transactions to the SCFM and maintain records on suspicious transactions and the people carrying them out for a period of five years. The legislation includes a "safe harbor" provision that protects reporting institutions from liability for cooperating with law enforcement agencies. In August 2003, the State Commission established the State Register of financial institutions, and by March 2007, the State Register contained information on 1,956 nonbank financial institutions.

Since November 2004, the GOU has made several efforts to pass a set of amendments to the AML laws in order to bring Ukraine's regime into compliance with FATF's revised Forty plus Nine recommendations. The Rada, or Parliament, twice rejected the government's draft in 2005. The government subsequently redrafted the law, narrowing its scope to the FATF recommendations, and omitting provisions introducing a new SCFM authority and other bureaucratic changes that had drawn opposition in the Parliament. The redrafted law passed in the second reading in June 2007, but was ultimately derailed by the lengthy political crisis of 2007.

In 2008, a new Parliament reintroduced the draft law, now entitled "On Amending Some Legislative Acts of Ukraine on Prevention to Legalization (Laundering) of the Proceeds from Crime and Terrorist Financing." On September 25, 2008, Parliament adopted the draft on the first reading. The main thrust of this new draft law is to broaden the types of entities and professionals that are subject to financial monitoring. The draft law will add lawyers and law firms, real estate firms, auditors, notaries, traders in precious metals, post offices (which can make money transfers), companies running lotteries, consulting companies and some other professionals to the list of obligated entities. The law will impose an affirmative obligation to report transactions that could be used for terrorist financing. The monitoring and regulation would be performed by the SCFM, along with the Ministries of Finance, Justice, Economy, and Transportation & Communication. The draft also provides some new mechanisms for stopping certain transactions believed to be tied to money laundering. The head of the SCFM claims the draft law is consistent with the 2003 FATF Forty plus Nine Recommendations. However, the law contains provisions that, while not formally in violation of FATF recommendations, do not fully address corruption issues. For example, the provision on financial monitoring of "politically exposed persons" applies only to international/foreign political persons and not to Ukrainian officials. The American Chamber of Commerce in Ukraine also has voiced concerns about the draft to Ukrainian authorities, arguing that it would greatly increase the authority of the SCFM without protecting the rights of the institutions subject to monitoring, and impose requirements on entities that are beyond the ability of such entities to fulfill.

It is unknown whether this session of the Rada will address the above draft law. It is not yet on Parliament's official agenda.

In 2004, authorities reduced the monetary threshold for compulsory financial monitoring from Ukrainian hryvnias (UAH) 300,000 (approximately $40,000) for cashless payments and UAH 100,000

(approximately $13,333) for cash payments, to UAH 80,000 (approximately $10,666) for payments using either method. The compulsory reporting threshold exists only if the transaction also meets one or more suspicious activity indicators as set forth by law. Any transaction suspected of being connected to terrorist activity must be reported to the appropriate authorities immediately.

Beginning in August 2005, as a result of amendments to the "Resolution on the Adoption of Instructions Regarding Movement of Currency, Precious Metals, Payment Documents, and Other Banking Documents over the Customs Border of Ukraine," travelers must declare cross-border transportation of cash sums exceeding $3,000, and name the origin of funds exceeding $10,000. Cash smuggling is substantial in Ukraine, although it is reportedly more related to unauthorized capital flight than to criminal proceeds or terrorist funding.

In 2005, the GOU sought to combat smuggling and corruption by reducing import duties, introducing new procedures for the Customs Service, and implementing transparent procedures for the privatization of state enterprises. Ukraine's 2005 budget eliminated the tax and customs duty privileges available in 11 Special Economic Zones (SEZs) and nine Priority Development Territories (PDTs) that operated within Ukraine, which had been associated with rampant evasion of customs duties and taxes. In late 2006, the government registered with the Parliament a draft law to restore tax and customs privileges for businesses operating in the SEZs. Additionally, a new draft Tax Code, also registered in Parliament, envisages tax and customs privileges for the zones. These drafts have remained in Parliament for some time, but have not been acted upon. Although legislation implementing this policy decision has not yet passed the Parliament, the GOU asserts the draft legislation includes provisions to avoid past problems associated with the zones.

Earlier AML laws are amended by Law 3163-IV, enacted in January 2006. Under the new law, the entities obligated to conduct initial financial monitoring must be able to provide proof they are fulfilling all Know Your Customer (KYC) identification requirements. The law also grants state agencies enhanced authority to exchange information internationally, improves rules on bank organization, and implements a screening requirement at the level of financial institutions. On September 14, 2006, Ukraine enacted amendments to the "Law on Banks and Banking" that require all banks to be formed as open joint-stock companies or as cooperatives. This measure strengthens disclosure requirements on the identity of the beneficial owners of banks. These amendments apply to all newly formed banks and provide a three-year period for existing banks to comply.

The SCFM, Ukraine's FIU, was established on December 10, 2001 by the Presidential Decree "Concerning the Establishment of a Financial Monitoring Department." The SCFM became operational on June 12, 2003. At that time, the SCFM was an independent authority administratively subordinate to the Ministry of Finance and the sole agency authorized to receive and analyze financial information from financial institutions. Effective January 1, 2005, Ukraine's Rada granted the SCFM the status of a central executive agency, subordinate to the Cabinet of Ministers rather than to the Ministry of Finance. The November 28, 2002 law "On Money Laundering Prevention," specifically states the SCFM is to operate free from political influences. However, a draft law "On the Opposition," which was submitted to the Parliament in early 2007, specifies that the parliamentary opposition could assign persons to certain leadership jobs in a number of state agencies, including the SCFM. Specifically, the draft law reserves the jobs of the director and two of the four deputy directors for nomination by the political opposition in the Parliament. Parliament adopted the draft in the first reading in 2007, but took no action on the draft in 2008. The law, if enacted, could free the FIU from the undue influence of one political party but could also contradict the November 2002, Law on Money Laundering Prevention by bringing the political process into play when making appointments to the affected positions. The director of the SCFM was replaced in February 2008, shortly after a new government came to power, but observers in Ukraine did not conclude that step was primarily politically motivated.

As of December 1, 2008, the SCFM has 25 local branches in Ukraine's regions. The SCFM is an administrative agency with no investigative or arrest authority. It is authorized to collect suspicious transaction reports (STRs) and analyze suspicious transactions, including those related to terrorist financing, and to transfer financial intelligence information to competent law enforcement authorities for investigation. The SCFM identifies possible cases for investigation by the Ministry of Interior, Tax Agency, State Security Agency and Prosecutor General's Office (PGO). The SCFM has processed, analyzed, and developed cases reportedly to the point of establishing the equivalent of probable cause prior to referral to law enforcement. The SCFM also has the authority to approve interagency agreements and exchange intelligence on financial transactions involving money laundering or terrorist financing with other FIUs. As of December 2008, the SCFM has signed memoranda of understanding (MOUs) with the FIUs of forty countries. It has become a regional leader with regard to the volume of case information exchanged with counterpart FIUs.

In 2007, the SCFM received 264,688 transaction reports, which include STRs and automatic threshold reports. The majority of these were submitted by banks. The SCFM designated approximately 25 percent of these for "active research" and sent 520 separate cases to law enforcement agencies. Of these cases, the SCFM referred 47 to the PGO, 169 to the State Tax Administration, 145 to the Ministry for Internal Affairs, and 159 to the State Security Service of Ukraine. As a result of subsequent investigation of these cases, law enforcement agencies initiated 271 formal criminal investigations (a 65 percent increase over the previous year), and submitted indictments in 40 of those cases (a five-fold increase). Between 2003 and 2007, 596 formal criminal investigations were opened, and indictments submitted in 60 of these cases. Convictions have been obtained in 28 of these cases. Although the reporting system is effective and the SCFM has generated a substantial number of cases, it did not lead to a significant number of convictions until 2007. From 2003-2006 there were convictions in only three cases, while in 2007, the number of cases jumped to 25.

Many observers believe the low prosecution and conviction rates are caused by reluctance at the PGO to follow up on the cases referred by the SCFM and by a lack of prosecutorial specialization. Local prosecutors may close money laundering investigations and cases prematurely or arbitrarily, possibly because of lack of sufficient manpower or resources, corruption, a weak understanding of money laundering crimes, or a belief that other types of crimes should take priority over money laundering.

Ukraine has been working with the European Commission and Council of Europe to increase its capacity to fight money laundering and terrorist financing since 2003. The ongoing Council of Europe project, which runs through April 2009, is focused on three areas: getting Ukraine's legislative framework up to international standards; enhancing the human capacities of key institutions and agencies; and developing the organizational and technical infrastructure of the system.

Ukraine has a general asset forfeiture regime, but this is largely an inappropriate and ineffective relic of Soviet-era legislation. Article 59 of the Ukrainian Criminal Code provides for the mandatory seizure of all or a part of the property of any person convicted for grave or particularly grave offenses, as defined in the code, regardless of whether this property bore any relation to the crime of conviction. With respect to money laundering, Article 209 allows for the forfeiture of criminally obtained money and other property. However, Ukraine lacks any functional regime for locating or seizing forfeitable assets. In particular, Ukraine lacks legislation allowing in rem forfeiture or the seizure of corporate assets, has no specialized asset forfeiture prosecutors or officials, and lacks any entity to administer forfeited assets. The GOU has drafted legislation aimed at improving the asset forfeiture regime and bringing it into compliance with international standards. The draft law has been completed by the Ministry of Justice, and is currently awaiting approval by the Cabinet of Ministers, for submission to Parliament.

On December 10, 2003, the Cabinet of Ministers issued Decree No. 1896, establishing a Unified State Information System of Prevention and Counteraction of Money Laundering and Terrorism Financing.

The system provides the SCFM with unobstructed access to the databases of 12 ministries and agencies, including the Ministry of Internal Affairs, Ministry of Economy, Ministry of Finance, State Tax Administration, State Security Service, State Customs Administration, State Property Fund, State Statistics Administration, Border Guard Service, Securities Commission, Financial Services Commission, and Control and Revision Department. The system became fully operational in December 2006. The SCFM leadership states it has unfettered access to all relevant information in the data bases of the aforementioned agencies.

The SCFM acknowledges the existence and use of alternative remittance systems in Ukraine, and its personnel have attended seminars and exchanged information about such systems. In 2007, the Security Service of Ukraine published a report signaling that hawala might be on the rise in Ukraine due to a large number of Ukrainians working abroad and the growth of foreign communities in Ukraine. The SCFM and security agencies monitor charitable organizations and other nonprofit entities that might be used to finance terrorism.

Law 3163-IV, which entered into force on January 1, 2006, enhances Ukraine's ability to exchange information internationally and places greater obligations on banks to combat terrorist financing. This law requires banks to adopt procedures to screen parties to all transactions using a SCFM-issued list of beneficiaries of, or parties to, terrorist financing. Banks must freeze assets for two days and immediately inform the FIU and law enforcement bodies whenever a party to a transaction appears on the list. The FIU can extend the freeze to five days. Banks developed their screening capabilities subsequent to implementation of the law. On October 25, 2006, the Cabinet of Ministers approved the SCFM's list, drawn from three sources: the United Nations 1267 Sanctions Committee's consolidated list; information from the Ukrainian Security Service on individuals and entities suspected of violating article 258 of the Ukrainian Criminal Code concerning terrorism; and the lists compiled by those countries that have bilateral agreements with Ukraine on mutual recognition of terrorist designations. On September 21, 2006, the Rada enacted revisions to Article 258 of the Criminal Code, adding Article 258-4 which explicitly criminalizes terrorist financing. The revised text mandates imprisonment from three to eight years for financing, material provision, or provision of arms with the aim of supporting terrorism. The revisions also amend the criminal procedure code to empower the State Security Service (SBU) with primary responsibility for investigating terrorist financing.

The GOU has cooperated with U.S. efforts to track and freeze the financial assets of terrorists and terrorist organizations. The NBU, the SCFM, the Securities Exchange Commission, the State Tax Administration, the SBU, and the Ministries of Finance, Internal Affairs, and Foreign Affairs are informed about the U.S. designation of suspected terrorists and terrorist organizations under Executive Order 13224 and other U.S. authorities. Through their regulatory agencies, banks and nonbank financial services also receive these U.S. designations and are instructed to report any transactions involving designated individuals or entities.

The U.S.-Ukraine Treaty on Mutual Legal Assistance in Criminal Matters was signed in 1998 and entered into force in February 2001. A bilateral Convention for the Avoidance of Double Taxation and the Prevention of Fiscal Evasion with Respect to Taxes on Income and Capital, which provides for the exchange of information in administrative, civil, and criminal matters, is also in force.

Ukraine is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Ukraine has signed, but not yet ratified, the UN Convention against Corruption. Ukraine is a member of MONEYVAL and also an observer and technical assistance donor to the Eurasian Group on Combating Money Laundering and the Financing of Terrorism (EAG), another FSRB. The SCFM is a member of the Egmont Group. It hosted working level meetings of the Egmont Group in Ukraine in October 2007.

Ukraine has strengthened and clarified its legislation and, with the SCFM, the NBU, and other actors in the financial and legal sectors, the Government of Ukraine has established a comprehensive AML regime. However, Ukraine's ability to implement this regime through consistent successful criminal prosecutions has yet to be proven. Ukraine should carefully review its pending draft laws to ensure they are in accordance not only with the language, but with the intent of international standards, and will not compromise the integrity of the FIU or any other supervisory bodies. Once such a review has been completed Ukraine should adopt the draft laws to bring noncovered entities within the scope of the anti-money laundering/counterterrorist financing laws. The GOU also should consider carefully the consequences of reestablishing tax and customs privileges that have been abused in the past. The GOU should take steps to improve implementation of its anti-money laundering/counterterrorist financing regime. The PGO should address the deficiencies of that office, such as a lack of specialization and limited professional experience with money laundering. Law enforcement agencies should give higher priority to investigating and prosecuting money laundering cases. Both law enforcement officers and the judiciary need a better understanding of the theoretical and practical aspects of investigating and prosecuting money laundering cases. Ukraine also should ratify the UN Convention against Corruption, and more aggressively address public corruption by investigating, prosecuting and convicting corrupt public officials.

United Arab Emirates

The United Arab Emirates (UAE) is an important financial center in the Gulf region. Dubai, in particular, is a major international banking and trading center. Although the financial sector is modern and progressive, the UAE remains a largely cash-based society. The country also has a growing offshore financial free zone. The UAE's robust economic development, political stability, and liberal business environment have attracted a massive influx of people, goods, and capital, which may leave the country susceptible to possible money laundering activities. The UAE is susceptible to money laundering due to its geographic location as the primary transportation and trading hub for the Gulf States, East Africa, and South Asia; longstanding trade relations with Iran; its expanding trade ties with the countries of the former Soviet Union; and lagging relative transparency in its corporate environment.

The potential for money laundering is exacerbated by the large number of resident expatriates (roughly 80—85 percent of total population) who send remittances to their homelands. Given the country's proximity to Afghanistan, where most of the world's opium is produced, narcotics traffickers are increasingly reported to be attracted to the UAE's financial and trade centers. Other money laundering vulnerabilities in the UAE include hawala, trade fraud, smuggling, the real estate boom, and the misuse of the international gold and diamond trade.

The Central Bank is responsible for supervising the UAE's financial sectors, which include banks, exchange houses, and investment companies. It is authorized to issue licenses and impose administrative sanctions for compliance violations. The Central Bank also has the authority to issue instructions and recommendations to financial institutions as it deems appropriate and to take any measures as necessary to ensure the integrity of the UAE's financial system. Following the September 11, 2001 terrorist attacks in the United States, and amid revelations that terrorists had moved funds through the UAE, the Emirates' authorities acted swiftly to address potential vulnerabilities. In close concert with the United States, the UAE imposed a freeze on the funds of groups with terrorist links, including the Al-Barakat organization, which was headquartered in Dubai. Both national and emirate-level officials have gone on record as recognizing the threat money laundering activities in the UAE pose to the nation's reputation and security. Since 2001, the UAE Government (UAEG) has taken steps to better monitor cash flows through the UAE financial system and to cooperate with international efforts to combat terrorist financing.

The UAE has enacted the Anti-Money Laundering Law No. 4/2002, and the Anti-Terrorism Law No. 1/2004. Both pieces of legislation, in addition to the Cyber Crimes Law No. 2/2006, serve as the foundation for the country's anti-money laundering and counterterrorist financing (AML/CTF) efforts. Law No. 4 of 2002 criminalizes all forms of money laundering activities. The law calls for stringent reporting requirements for wire transfers exceeding 2000 dirhams (approximately $545) and currency imports above 40,000 dirhams (approximately $10,900). The law imposes criminal penalties for money laundering that includes up to seven years in prison plus a fine of up to 300,000 dirhams (approximately $81,700), as well as a seizure of assets upon conviction. The law also provides safe harbor provisions for reporting officers.

Prior to the passage of the Anti-Money Laundering Law, the National Anti-Money Laundering Committee (NAMLC) was established in July 2000 to coordinate the UAE's anti-money laundering policy. The NAMLC was later codified as a legal entity by Law No. 4/2002, and is chaired by the Governor of the Central Bank. Members of the NAMLC include representatives from the Ministries of Interior, Justice, Finance, and Economy, the National Customs Board, Secretary General of the Municipalities, Federation of the Chambers of Commerce, and five major banks and money exchange houses, as observers.

Administrative Regulation No. 24/2000 provides guidelines to financial institutions for monitoring money laundering activity. This regulation requires banks, money exchange houses, finance companies, and any other financial institutions operating in the UAE to follow strict "know your customer" guidelines. Financial institutions must verify the customer's identity and maintain transaction details (i.e., name and address of originator and beneficiary) for all exchange house transactions over the equivalent of $545 and for all non-account holder bank transactions over $10,900. The regulation delineates the procedures to be followed for the identification of natural and juridical persons, the types of documents to be presented, and rules on what customer records must be maintained on file at the institution. Other provisions of Regulation 24/2000 call for customer records to be maintained for a minimum of five years and further require that they be periodically updated as long as the account is open. In 2008, the UAE Central Bank issued a circular instructing banks and exchange houses to obtain certain identity and transaction information for all cash exchange transactions over $545 and outlining additional procedures for bank transfers in excess of $953. In July 2004, the UAE government strengthened its legal authority to combat terrorism and terrorist financing by passing Federal Law Number No. 1/2004. The Law specifically criminalizes the funding of terrorist activities and terrorist organizations. It sets stiff penalties for the crimes covered, including life imprisonment and the death penalty. It also provides for asset seizure or forfeiture. Under the law, founders of terrorist organizations face up to life imprisonment. The law also penalizes the illegal manufacture, import, or transport of "nonconventional weapons" and their components that are intended for use in a terrorist activity.

Article 12 provides that raising or transferring money with the "aim or with the knowledge" that some or all of this money will be used to fund terrorist acts is punishable by "life or temporary imprisonment," regardless whether the terrorist acts occur. Law No. 1/2004 grants the Attorney General (or his deputies) the authority to order the review of information related to the accounts, assets, deposits, transfer, or property movements on which the Attorney General has "sufficient evidence to believe" are related to the funding or committing of a terror activity as defined in the law. In 2008, the UAE Ministry of Justice issued two circulars instructing lawyers and federal court clerks to report to the UAE Anti-Money Laundering and Suspicious Case Unit (the financial intelligence unit) any commercial or financial agreements suspected of links to terrorism, terrorist finance or terrorist organizations.

The law also provides for asset seizure and confiscation. Article 31 gives the Attorney General the authority to seize or freeze assets until the investigation is completed. Article 32 confirms the Central Bank's authority to freeze accounts for up to seven days if it suspects that the funds will be used to

fund or commit any of the crimes listed in the law. The law also allows the right of appeal to "the competent court" of any asset freeze under the law. The court will rule on the complaint within 14 days of receiving the complaint. Law No. 1/2004 also established the "National Anti-Terror Committee" (NATC) to serve as the government's interagency liaison with respect to implementing the United Nations Security Council Resolutions (UNSCR) on terrorism, and sharing information with its foreign counterparts as well as with the United Nations. Representatives from Ministries of Foreign Affairs, Interior, Justice, and Defense; Central Bank; State Security Department; and Federal Customs Authority comprise the NATC.

The Central Bank also states that it circulates an updated UNSCR 1267 Sanctions Committee's consolidated list of suspected terrorists and terrorist organizations to all the financial institutions under its supervision. In 2007, the UAE took steps toward fulfillment of its UN nonproliferation obligations. On August 31, 2007 the UAE issued Law No. 13 of 2007 on export and import controls; the law is currently under amendment. With regard to the UAE's UNSCR 1737 and 1747 commitments, the UAE Central Bank has ordered banks and other financial institutions to freeze accounts or deposits of designated entities. It also has ordered financial institutions to cease transfers on behalf of designated entities and to refrain from entering into new commitments for grants, financial assistance, and concession loans to the Iranian Government.

The Anti-Money Laundering and Suspicious Case Unit (AMLSCU) was established in 2002 as the UAE's financial intelligence unit (FIU), and was housed within the Central Bank. In addition to receiving Suspicious Transaction Reports (STRs), the AMLSCU is authorized to send information requests to foreign regulatory authorities to conduct its preliminary investigations based on suspicious transaction report data. The AMLSCU joined the Egmont Group in June 2002. The AMLSCU reports that it has issued a total of 42 freeze orders in response to STRs between December 2000 (prior to the establishment of the FIU) and October 2006. The 2008 MENAFATF Mutual Evaluation of the UAE noted that STR reporting requirements warranted additional clarity with regard to the level of suspicion of money laundering activity needed to require filing a report with the FIU. The result was that, as of 2006, the latest year for which the Central Bank would supply figures, less than 500 STRs were filed by a relatively small number of core banks. The mutual evaluation team considered this number low for the UAE's level of financial activity.

International Monetary Fund (IMF) conducted an assessment of the UAE financial system in 2007. The report concluded that the government of the UAE is in the midst of implementing an important agenda for further strengthening the country's banking system and its prudential and regulatory oversight. The report contains no information on the UAE compliance with the FATF's 40 plus 9 recommendations. In August 2008, the UAE Central Bank Governor announced that the UAE had implemented 80 percent of the measures demanded by IMF.

It is unclear how many money laundering prosecutions have taken place in the UAE in 2008. However, there were two high profile money laundering cases in the UAE during the 2006/2007 timeframe and another major case in 2008. In November 2007, the Sharjah Appeals Court upheld a verdict sentencing seven men to five years in prison for money laundering. An Abu Dhabi court also sentenced two of the individuals to life imprisonment for drug trafficking and the rest to ten year sentences for drug trafficking. The individuals were arrested in 2006 for attempting to smuggle 2.5 tons of hashish from Pakistan to Holland, via Sri Lanka, the UK, and Belgium. UAE authorities worked with law enforcement officials in the respective countries to track the shipment. In October 2007, the Dubai police referred 48 suspects to the Public Prosecutors on charges of money laundering and abetting drug trafficking. In June 2008, the Dubai Attorney General referred a Dutch and an Arab national to the Dubai Court of Misdemeanors for allegedly laundering 60 million dirhams (approximately $16.33 million) in drug trafficking proceeds through two front companies in Dubai. It should be noted that the investigations related to many of the high profile money laundering cases

have been carried out by the small Anti Money Laundering Unit of the Dubai Police rather than by the AMLSCU.

Several amendments were made to the Central Bank Regulations 24/2000 in July 2006. First, the regulations added the term "terrorist financing" to any references made to the term "money laundering." Second, the regulations required financial institutions to freeze transactions that they believe may be destined for funding terrorism, terrorist organizations, or for terrorist purposes. The regulations also require financial institutions to notify the AMLSCU in writing of such transactions "in case of any doubt." Finally, enhanced due diligence requirements for charities were promulgated, requiring banks to obtain a certificate from the Minister of Social Affairs before opening or maintaining any charitable organization-type account.

In 2006, the UAE enacted Law No. 2/2006 of the Cyber Crimes. Article 19 of the law criminalized the electronic transfer of money or property through the Internet in which the true sources of such assets are either concealed or linked to criminal proceeds. Violations are punishable by up to seven years imprisonment and fines ranging from $8,170 to $54,500. Article 21 of the law outlaws the use of the Internet to finance terrorist activities, promote terrorist ideology, disseminate information on explosives, or to facilitate contact with terrorist leaders. Any violation of Article 21 is punishable by up to 5 years imprisonment.

Hawala is where money laundering activity is likely more prevalent due to the largely undocumented nature of this informal remittance system. Dubai is a regional hawala center. Hawala is an attractive mechanism for terrorist and criminal exploitation due to its lack of transparency to law enforcement and regulators and the highly resilient nature of the system. In 2003, the Central Bank issued new regulations to help improve the oversight of hawala, including registration of hawala brokers (hawaladars). The new regulations required hawaladars to submit the names and addresses of all originators and beneficiaries of funds and to file suspicious transaction reports on a monthly or quarterly basis. However, since the inception of the program, there reportedly have not been any suspicious reports filed by hawaladars.

As of April 2008, the Central Bank had registered 265 hawaladars, with an additional 104 applicants working to complete their registration requirements. Once registered, the Central Bank conducts one-on-one training sessions with each registered hawaladar to ensure that dealers understand the record-keeping and reporting obligations. The registered hawaladars are required to use an account they open at the Central Bank to process their transactions. Currently, there is no accurate estimate of the total number of UAE-based hawala brokers, and there is no penalty for failure of hawaladars to register with the Central Bank. Officials argue that the registration program is still in the initial phase of determining the magnitude of the industry.

The UAE has not set any limits on the amount of cash that can be imported into or exported from the country. No reporting requirements exist for cash exports. However, the Central Bank requires that any cash imports over the equivalent $10,900 must be declared to Customs; otherwise undeclared cash may be seized upon attempted entry into the country. All cash forfeiture cases are handled at the judicial level because there are no administrative procedures to handle forfeited cash. Still, enforcement mechanisms are lax. Customs officials, police, and judicial authorities tend to not regard large cash imports as potentially suspicious or criminal type activities, arguing that the UAE is a cash-based economy, and it is not unusual for people to carry significant sums of cash.

Dubai remains the center of the UAE's burgeoning diamond trade, although new facilities are springing up in the Emirate of Ras Al Khaimah as interest spreads in the lucrative business. The UAE has been a participant in the Kimberley Process Certification Scheme for Rough Diamonds since November 2002, and began certifying rough diamonds exported from the UAE on January 1, 2003. Law No. 13 of 2004 regulates supervision of Import/Export and Transit of Rough Diamonds. Article 5

of the law prohibits the import of rough diamonds, unless they are accompanied by a Kimberley Process certificate and in a sealed, tamper resistant container.

The Dubai Diamond Exchange (DDE), a subsidiary of the Dubai Multi Commodities Center (DMCC), is a quasi-governmental organization charged with issuing Kimberley Process (KP) certificates in the UAE. Prior to January 1, 2003, the DMCC circulated a sample UAE certificate to all KP participant states and embarked on a public relations campaign to familiarize the then estimated 50 diamond traders operating in Dubai with the new KP requirements. There are more than 300 firms involved in diamond trading in Dubai. Under the KP regulations, UAE Customs is the sole point of entry for both rough and finished diamonds to the UAE. Customs officials are authorized to delay or even confiscate those diamonds entering the UAE that do not have the proper certificates.

In October 2008, Dubai International Airport customs officials detained an African woman who had uncut diamonds valued at over $ 1 million concealed on her body. In 2006, Russian customs officials reportedly apprehended an air passenger from Dubai after he tried to smuggle 2.5 kilos of diamonds into the country. There are also reports that diamonds are increasingly being used as a medium to provide counter valuation in hawala transfers, particularly between Dubai and Mumbai.

The former head of the Dubai Diamond Exchange implemented enhanced monitoring measures in compliance with the Moscow Resolution on Cote d'Ivoire of November 2005, but two suspect diamond shipments of questionable provenance released by the DDE in 2006 and 2007 indicate continuing weaknesses in the process. The UN Group of Experts on Cote d'Ivoire, visiting Dubai in May 2007, raised with the DDE the release in September 2006 and January 2007, respectively, of two shipments of diamonds with suspect Ghanaian certificates of origin. In both cases the World Diamond Council was requested to verify the origin of the diamonds. In the first instance the Working Group of Diamond Experts concluded that the assessed diamonds bore characteristics unknown in Ghanaian diamonds, but possibly consistent with stones from Guyana or Brazil. In the second case, the diamonds were released before the WDC's final report was released. The UN Group of Experts on Cote d'Ivoire also reported that individuals in Dubai's Gold Land stated that they had in their possession large quantities of African diamonds without Kimberley Process certification.

In May 2008, the UAE and Russia signed an executive plan for enforcement of the Anti-Crime Cooperation Agreement, which was inked between the two countries in September 2007. The plan called for cooperation and information exchange in the fields of counterterrorism, prevention of organized crimes, money laundering, financial crimes, crimes associated with transport, smuggling of drugs and other forms of dangerous crimes.

The Securities and Commodities Authority (SCA) supervises the country's two stock markets. In February 2004, the SCA issued anti-money laundering guidelines to all brokers that included identity verification instructions for new customer accounts, a reporting requirement for cash transactions above U.S. $10,900, and a minimum five-year record keeping requirement for all customer account information. The SCA also instructed brokers to file suspicious transaction reports with the SCA for initial analysis before they are forwarded to the AMLSCU for further action.

The UAE's real estate market continues to grow with the various emirates following Dubai's model of opening up some property ownership to expatriates. Dubai's real estate market grew significantly in 2008, with a slump later in the year due to the global economic downturn. The sector is susceptible to money laundering abuse. In 2002, Dubai began to allow three real estate companies to sell "freehold" properties to noncitizens. Since then, several other emirates have followed suit. For instance, Abu Dhabi has passed a property law, which provides for a type of lease-hold ownership for noncitizens. In addition, citizens of GCC countries have the right to purchase and trade land within designated investment areas, while other expatriates are permitted to invest in real estate properties for a 99-year leasehold basis. Due to the intense interest in and reported cash purchases of such properties, the potential for money laundering has become of increased concern to the UAE Government. As a result,

developers have stopped accepting cash purchases for these properties. The UAE does not have a central database to show registered property owners within the UAE, which encumbers international money laundering investigations.

Since the September 11, 2001 terrorist attacks, the UAE Government (UAEG) has been more sensitive to regulating charitable organizations and accounting for funds transfers abroad. In 2002, the UAEG mandated that all licensed charities interested in transferring funds overseas must do so via one of three umbrella organizations: the Red Crescent Authority, the Zayed Charitable Foundation, or the Muhammad Bin Rashid Charitable Trust. These three quasi-governmental bodies are in a position to ensure that overseas financial transfers go to legitimate parties. As an additional step, the UAEG has contacted the governments in numerous aid receiving countries to compile a list of recognized acceptable recipients for UAE charitable assistance.

Charities are regulated by the UAE Ministry of Social Affairs, which is responsible for licensing and monitoring registered charities in these emirates. The Ministry also requires these charities to keep records of all donations and beneficiaries, and to submit financial reports annually. Charities in Dubai are licensed and monitored by the Dubai Department of Islamic Affairs and Charitable Activities. Some charities, however, particularly those located in the Northern Emirates, are only registered with their local emirate authority and not the federal Ministry. In July 2006, Regulation 24/2000 was amended, requiring charities from all emirates to obtain a certificate from the Minister of Social Affairs before being permitted to open or maintain bank accounts in the UAE. This amendment effectively required that all charities must be registered federally and no longer at just the emirate level. In November 2006, the UAE hosted a United Kingdom/Gulf Cooperation Council conference on charities, and made a proposal to hold biannual meetings going forward with the UK and GCC on charities oversight.

The UAE has both free trade zones (FTZs) and one financial free zone (FFZ). The number of FTZs is growing, with 37 operating in the UAE. Every emirate except Abu Dhabi has at least one functioning FTZ. The free trade zones are monitored by the local emirate rather than federal authorities.

There are over 5,000 multinational companies located in the FTZs, and thousands more individual trading companies. The FTZs permit 100 percent foreign ownership, no import duties, full repatriation of capital and profits, no taxation, and easily obtainable licenses. Companies located in the free trade zones are considered offshore or foreign entities for legal purposes. However, UAE law prohibits the establishments of shell companies and trusts, and does not permit nonresidents to open bank accounts in the UAE. The larger FTZs in Dubai (such as Jebel Ali free zone) are well-regulated. Although some trade-based money laundering undoubtedly occurs in the large FTZs, a higher potential for financial crime exists in some of the smaller FTZs located in the northern emirates.

In March 2004, the UAEG passed Federal Law No. 8, regarding the Financial Free Zones (FFZs) (Law No. 8/2004). Although the new law exempts FFZs and their activities from UAE civil, and commercial laws, FFZs and their operations are still subject to federal criminal laws including the Anti-Money Laundering Law (Law No. 4/2002) and the Anti-Terror Law (Law No. 1/2004). As a result of Law 8/2004 and a subsequent federal decree, the UAE's first financial free zone (FFZ), known as the Dubai International Financial Center (DIFC), was established in September 2004. By September 2005, the DIFC had opened its securities market, the Dubai International Financial Exchange (DIFX).

Law No. 8/2004 limits the issuance of licenses for banking activities in the FFZs to branches of companies, joint companies, and wholly owned subsidiaries provided that they "enjoy a strong financial position and systems and controls, and are managed by persons with expertise and knowledge of such activity." The law prohibits companies licensed in the FFZ from dealing in UAE currency (i.e., dirham), or taking "deposits from the state's markets." Further, the law stipulates that the licensing standards of companies "shall not be less than those applicable in the state." The law

empowers the Emirates Stocks and Commodities Authority to approve the listing of any company listed on any UAE stock market in the financial free zone, as well as the licensing of any UAE stock broker. Insurance activities conducted in the FFZ are limited by law to reinsurance contracts only. The law further gives competent authorities in the Federal Government the power to inspect financial free zones and submit their findings to the UAE cabinet.

In 2007 the Cabinet issued Resolution No. 28 that provided implementing regulations for financial free zones. The regulations specify that FFZs submit their semi-annual reports on activities and compliance to the UAE Cabinet. The regulations also spell out that inspections of FFZs will be carried out by cabinet resolution through a ministerial committee. These inspections will be carried out in cooperation with the FFZs. Results will be referred to the cabinet for action. The Regulation also instructs the FFZs to enter into Memorandums of Understanding (MOUs) with relevant authorities, such as the Central Bank, the Ministry of Economy, the Securities and Commodities Authority, and the Insurance Authority, for the purposes of better coordination, cooperation, and control.

DIFC regulations provide for an independent regulatory body, namely the Dubai Financial Services Authority (DFSA), to report its findings directly to the office of the Dubai ruler and an independent Commercial Court. According to DFSA regulators, the DFSA due diligence process is a risk-based assessment that examines a firm's competence, financial soundness, and integrity. Prior to the inauguration of the DIFC in 2004, several observers called into question the independence of the DFSA as a result of the high profile firings of the chief regulator and the head of the regulatory council (i.e., the supervisory authority). Subsequent to the firings, Dubai passed laws that gave the DFSA more regulatory independence from the DIFC, although these laws have not yet been tested. The DFSA, who modeled its regulatory regime after the United Kingdom, is the sole authority responsible for issuing licenses to those firms providing financial services in the DIFC.

The DFSA supervises and regulates a total of 299 entities: 232 authorized firms, 49 ancillary services providers, 16 registered auditors and 2 markets. The DFSA prohibits offshore casinos or Internet gaming sites in the UAE, and requires firms to send suspicious transaction reports to the AMLSCU (along with a copy to the DFSA). To date, there have been 30 suspicious transaction reports issued from firms operating in the DIFC (seven in 2008). Although firms operating in the DIFC are subject to Law No. 4/2002, the DFSA has issued its own anti-money laundering regulations and supervisory regime, which has caused some ambiguity about the Central Bank's and the AMLSCU's respective authorities within the DIFC. Ongoing discussions continue between the DFSA and the UAE Central Bank to create a formal bilateral arrangement.

As a result, the DIFC acknowledged the need to enhance its regulatory and compliance authority. On July 18, 2007, it enacted regulations for nonfinancial Anti-Money Laundering Anti Terrorist Finance which applies Financial Action Task Force (FATF) compliant requirements in the DIFC jurisdiction to real estate agents, dealers in precious metals and stones, dealers in high value goods (cash payments of over the equivalent of $15,000), non-Authorized Service Providers, lawyers, accountants, auditors, and non-DFSA regulated Trust and Company Service Providers. These regulations do not apply to DFSA regulated firms. With regard to auditors and accountants, for example, this would apply to those that do not audit authorized firms. In January 2008, DFSA issued a notice to authorized firms, authorized market institutions, and ancillary service providers highlighting 2007 FATF guidance on financial prohibitions with respect to Iran.

The DFSA has undertaken a campaign to reach out to other international regulatory authorities to facilitate information sharing. As of November 2008, the DFSA has MOUs with 41 other regulatory bodies, including the UK's Financial Services Authority (FSA), the Emirates Securities and Commodities Authority, and the U.S. Commodity Futures Trading Commission (CFTC). On October 23, 2007, the DFSA entered into a MOU with the five U.S. banking supervisors.

In September 2008, the IMF issued n a 250-page report on the UAE's anti-laundering efforts. While the UAE was among the first Arab countries to enforce anti-laundering legislation, the report stated that the UAE's laws need to be amended to block loopholes, cope with changes and match international standards. The IMF also recommended the UAE increase human and material resources, given the rapid expansion in the country's free zones and an influx of foreign capital into these zones. Following publication of the report, the UAE Federal Customs Authority (FCA) acknowledged that more needs to be done to standardize customs laws and enforcement across UAE to curb money laundering and that the agency is working to comply with IMF recommendations.

The UAE is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Corruption, and the UN Convention against Transnational Organized Crime. The UAE is a member of the Middle East and North Africa Financial Action Task Force (MENAFATF).

The Government of the UAE has shown some progress in enhancing its AML/CTF program. Information sharing between the AMLSCU and foreign FIUs has substantially improved. However, several areas requiring further action by the UAEG remain. Law enforcement and customs officials need to proactively recognize money laundering activity and develop cases based on investigations, rather than wait for case referrals from the AMLSCU that are based on SARs. Additionally, law enforcement and customs officials should conduct more thorough inquiries into large and undeclared cash imports into the country, as well as require—and enforce—outbound declarations of cash and gold. All forms of trade-based money laundering must be given greater scrutiny by UAE customs and law enforcement officials, including customs fraud, the trade in gold and precious gems, commodities used as countervaluation in hawala transactions, and the misuse of trade to launder narcotics proceeds. The UAE should increase the resources it devotes to investigation of AML/CTF both federally at the AMLSCU and at emirate level law enforcement. Moreover, per observations in the 2008 MENAFATF mutual evaluation of the UAE, the absence of meaningful statistics across all sectors is a significant hindrance to the assessment of the effectiveness of the AML/CTF program. The Central Bank should move from the initial phase of hawaladar registration to compliance and enforcement coupled with investigations. The cooperation between the Central Bank and the DFSA needs improvement, and lines of authority need to be clarified. Cabinet Resolution No. 28 of 2007 should help in this regard. The UAE should conduct more follow-ups with financial institutions and the MSA regarding the recent tightening of regulations on charities to ensure their registration at the federal level. The UAE should also continue its regional efforts to promote sound charitable oversight, and engage in a public campaign to ensure all local charities are aware of registration requirements.

United Kingdom

The United Kingdom (UK) plays a leading role in European and world finance and remains attractive to money launderers because of the size, sophistication, and reputation of its financial markets. Although narcotics are still a major source of illegal proceeds, the proceeds of other offenses, such as financial fraud and the smuggling of people and goods, have become increasingly important. The past few years have witnessed the movement of cash placement away from banks and mainstream financial institutions as these entities have tightened their controls and increased their vigilance. The use of bureaux de change, cash smugglers (into and out of the UK), and traditional gatekeepers (including solicitors and accountants) to move and launder criminal proceeds has been increasing since 2002.

Also on the rise are credit and debit card fraud and the purchasing of high-value assets to disguise illegally obtained money. In 2007, total card fraud losses increased by 25 percent to £535 million (approximately $936,250,000). However, over the past three years losses on mainstream card transactions have fallen by 67 percent, due largely to the use of the chip and PIN system. Counterfeit card fraud increased overall by 46 percent to £144.3 million (approximately $252,530,000) in 2007,

primarily due to criminals copying British cards and using them in countries which do not yet have the chip and PIN system. The main area of credit card fraud to rise in 2007 was card-not-present (CNP) fraud, which increased by 37 percent in 2007, compared to 2006. However, the number of people and retailers offering online and telephone shopping have also hugely increased in the same period.

Criminal proceeds are mostly generated in the large metropolitan areas by drug-traffickers and other domestic criminals. Cities such as London, Liverpool and Birmingham have large drug markets and also serve as supply points for markets in smaller cities and towns, drawing in significant flows of illicit cash. Additionally, according to a Home Office estimate published by the Serious Organized Crime Agency (SOCA), the markets for illegal goods and services as well as criminal abuse of legitimate markets in the UK generate about £15 billion (approximately $26,250,000,000) in revenue per annum for organized crime. Businesses that are particularly attractive to criminals are those with high cash turnovers and those involved in overseas trading.

Illicit cash is consolidated in the UK, and then moved overseas. Traffickers make extensive use of money service businesses (MSBs), cash smuggling, and alternative remittance systems to remove cash from the UK. Because dealers in the UK generally collect cash, most traffickers are left with excess small currency, usually £10 notes. This has led to the creation of cash smuggling operations to move large sums of sterling out of the country. The SOCA analysis suggests that more sterling has exited the UK in recent years than entered due to the relative ease of converting sterling in other countries. Cash can be smuggled via courier, freight or post, and moved through the various points of exit from the UK. Heroin proceeds from the UK are often laundered through Dubai en route to traffickers in Pakistan and Turkey. Cocaine proceeds are frequently repatriated to South America via Jamaica and Panama.

Narcotics-related money laundering has been a criminal offense in the UK since 1986. The laundering of proceeds from other serious crimes is criminalized by subsequent legislation. The Proceeds of Crime Act 2002 (POCA) creates a new criminal offense, applicable to all regulated sectors, of failing to disclose suspicious transactions in respect to all crimes, not just "serious," narcotics- or terrorism-related crimes, as had previously been the rule. The POCA also expands investigative powers relative to large movements of cash. Sections 327 to 340 of the Act address possession, acquisition, transfer, removal, use, conversion, concealment or disguise of criminal or terrorist property, inclusive of, but not limited to, money. The POCA also criminalizes tipping off. The "Money Laundering Regulations 2003," along with amending orders for the POCA and the Terrorism Act, impose requirements on various entities, including attorneys, and introduce a client identification requirement and requirements for internal reporting procedures and training.

The Fraud Act 2006, which took effect on 15 January 2007, brings significant changes to offenses in the fraud and forgery offense group. Changes are also made to the way in which the police record fraud offenses. In October 2008, the National Fraud Strategic Authority was launched as an Executive Agency of the Attorney General's Office to coordinate activity across the whole economy, both the private and public sectors, in order to offer further protection of the economy against fraud.

Banks and nonbank financial institutions in the UK must report suspicious transactions. In 2001, money laundering regulations were extended to MSBs, and in September 2006, the Government of the United Kingdom (GOUK) published a review of the regulation and performance of MSBs in preventing money laundering and terrorist financing. Since 2004, more business sectors are subject to formal suspicious activity reporting (SAR) requirements, including attorneys, solicitors, accountants, real estate agents, and dealers in high-value goods, such as cars and jewelry. Sectors of the betting and gaming industry that are not currently regulated are being encouraged to establish their own codes of practice, including a requirement to disclose suspicious transactions.

Following an extensive consultation period, Her Majesty's Treasury published new Money Laundering Regulations which took effect December 15, 2007. The regulations introduce a

comprehensive requirement to identify and provide an extensive definition of the beneficial owner; and introduce explicit requirements to apply enhanced due diligence, plus additional steps, when dealing with politically exposed persons. Correspondent banking relationships with shell banks are banned; and regulated firms, including designated nonfinancial businesses, are provided a legally sanctioned 'safe harbor' when they comply with HM Treasury approved guidance. The 2007 Regulations also give the UK Gambling Commission the power to supervise casinos, ensuring their compliance with the obligations placed on the physical and virtual casino sectors in the UK, including appropriate customer due diligence requirements.

European Union Council Regulation No. 1889/2005, known as the "Cash Controls Regulation," became applicable in the UK on June 15, 2007. This regulation mandates a cash declaration system for every person entering or exiting the EU with cash of 10,000 euros (approximately $13,500) or its equivalent in other currencies. The UK employs a written declaration system.

The UK's banking sector provides accounts to residents and nonresidents, who can open accounts through various intermediaries that often advertise on the Internet and also offer various offshore services. Individuals typically open nonresident accounts for tax advantages or for investment purposes. Private banking constitutes a significant portion of the British banking industry. Both resident and nonresident accounts are subject to the same reporting and record keeping requirements.

Bank supervision is the responsibility of the Financial Services Authority (FSA). The FSA's primary responsibilities relate to the safety and soundness of the institutions under its jurisdiction, however, it also plays an important role in the fight against money laundering through its continued involvement in the authorization of banks and investigations of money laundering activities involving banks. The FSA regulates some 29,000 firms, including European Economic Area (EEA) firms "passporting" into the UK (firms doing business on a cross-border basis), ranging from global investment banks to very small businesses, and around 165,000 individuals. It also regulates mortgage and general insurance agencies, totaling over 30,000 institutions. The FSA administers a civil-fines regime and has prosecutorial powers. It also has the power to make regulatory rules with respect to money laundering and to enforce those rules with a range of disciplinary measures (including fines) if the institutions fail to comply. In October 2006, the financial services sector adopted National Occupational Standards of Competence in the fields of compliance and anti-money laundering.

The Serious Organized Crime and Police Act of 2005 (SOCAP) amends the money laundering provisions in the POCA. Under the SOCAP, foreign acts are no longer considered money laundering if they do not violate the law in the foreign jurisdiction. SOCAP also creates the SOCA, which houses the UK's financial intelligence unit (FIU). In 2006, SOCA assumed all FIU functions from the National Criminal Intelligence Service (NCIS). SOCA has three functions: the prevention and detection of serious organized crime; the mitigation of the consequences of such crime; and the function of receiving, storing, analyzing and disseminating information, including SARs. Under the law, SOCA's functions are not restricted to serious or organized crime but are applicable to all crimes, and those functions include assistance to other agencies in their enforcement responsibilities. The number of SARs received dipped from 220,484 SARs during the year ending September 30, 2007, to 210,524 during the most recent reporting period of October 2007—September 2008. During the current reporting period, 956 SARS were referred to the National Terrorist Finance Investigation Unit, as compared to 1,088 in the period ending September 2007.

The POCA enhances the efficiency of the forfeiture process and increases the recovered amount of illegally obtained assets by consolidating existing laws on forfeiture and money laundering into a single piece of legislation, and, perhaps most importantly, creating a civil asset forfeiture system for the proceeds of unlawful conduct. The Assets Recovery Agency (ARA), established to enhance financial investigators' power to request client information from a bank, is a product of this legislation. The Act provides for confiscation orders and for restraint orders to prohibit dealing with

property. It also allows for recovery of property obtained through or used for unlawful conduct. Furthermore, the Act shifts the burden of proof to the holder of the assets to prove the assets were acquired through lawful means. In the absence of such proof, assets may be forfeited, even without a criminal conviction. The Act gives standing to overseas requests and orders concerning property believed to be the proceeds of criminal conduct. The POCA also gives greater powers of seizure at a lower standard of proof. In light of this, Her Majesty's Revenue and Customs increased its national priorities to include investigating the movement of cash through money exchange houses and identifying unlicensed money remitters. The Serious Crime Act 2007 merges the ARA's operational arm with SOCA and ARA's training function with the National Policing Improvement Authority. It also extends the powers of civil recovery to wider prosecution authorities and the powers of cash seizure to a wider range of law enforcement bodies. In its 2007/2008 annual report as of March 31, 2008, SOCA noted that 41 Financial Reporting Orders had been imposed, resulting in reports on convicted criminals' finances being received and scrutinized; omissions detected and appropriate action taken. The total value of assets recovered by all agencies in England, Wales, and Northern Ireland reached over £185 million (approximately $296,000,000) over three years.

In an illustrative case, agencies looked into the activities of UK-based criminals who used the internet to trade stolen bank, credit card, and identity information using a website they had created. The agencies were able to identify the offenders and arrested, prosecuted, and convicted involved UK citizens. The potential loss to the UK financial sector from the actions of just one of the conspirators was estimated in excess of £6 million (approximately $9,600,000). Another investigation targeted an organized group of money launderers operating in the UK but controlled from Dubai and Pakistan. They used hawala to eventually move drug money between the UK, Pakistan and Dubai, among other countries. The UK end of the organization provided laundering services to UK drug dealers. Records seized showed that almost £15 million (approximately $26,250,000) in cash had been passed. In September 2007, the last of eight men was sentenced. The main defendant received ten years imprisonment; the eight defendants together received 39 years for money laundering.

The Terrorism (United Nations Measures) Order 2001 makes it an offense for any individual to provide financial or related services, directly or indirectly, to or for the benefit of a person who commits, attempts to commit, facilitates, or participates in the commission of acts of terrorism. The Order also makes it an offense for a covered entity to fail to disclose to Her Majesty's Treasury a suspicion that a customer or entity is attempting to participate in acts of terrorism. The Anti-Terrorism, Crime, and Security Act 2001 provides for the freezing of assets.

The UK's new terrorism legislation, the Counter-Terrorism Act 2008, entered into force on November 26, 2008. The new law grants the UK further authority to gather and share information for counterterrorism and other purposes, and to act against terrorist financing, money laundering, and certain other activities. The Act also amends the definition of "terrorism," and amends previous legislation relating to terrorist offences, control orders and the forfeiture of terrorist cash. Under the new law, the UK has the authority to impose measures on private sector actors that do business with non-EEA countries (1) against which the Financial Action Task Force (FATF) has applied countermeasures; (2) that HM Treasury has determined pose a money laundering or terrorist financing risk; or (3) that have developed or facilitated weapons of mass destruction that pose a risk to the UK.

As a direct result of the events of September 11, 2001, NCIS established a separate National Terrorist Financing Investigative Unit (NTFIU), controlled by the Metropolitan Police Services (MPS, also known as "Scotland Yard") to maximize the effect of reports from the regulated sector. The NTFIU chairs a law enforcement group to provide outreach to the financial industry concerning requirements and typologies. The operational unit that responds to the work and intelligence development of the NTFIU has seen a threefold increase in staffing levels directly due to the increase in the workload. The MPS has responded to the growing emphasis on terrorist financing by expanding the focus and strength of its specialist financial unit dedicated to this area of investigations.

In the UK, HM Treasury implements UN financial sanction regimes using its powers under the relevant Order in Council, and those sanctions are enforced by the Treasury's Asset Freezing Unit. Individuals and organizations who have been listed by the UN Sanctions Committee or who are suspected of committing or facilitating terrorist acts, are listed on the sanctions page on its website. UK financial institutions are immediately alerted to changes to lists. UK banks and financial institutions are legally obliged to freeze the funds of all those individuals and organizations whose names appear on the lists.

Charitable organizations and foundations are subject to supervision by the UK Charities Commission. Such entities must be licensed and are subject to reporting and record keeping requirements. The Commission has investigative and administrative sanctioning authority, including the authority to remove management, appoint trustees and place organizations into receivership. The GOUK reviewed regulation of the charitable sector in January 2008; the review formed the basis of a new Charities Commission strategy, including practical and regulatory changes to strengthen the safeguards against terrorist abuse of the charitable sector.

The UK is a party to the 1988 UN Drug Convention, the UN Convention against Corruption, the UN Convention against Transnational Organized Crime, and the UN Convention for the Suppression of the Financing of Terrorism. The UK is a member of the Financial Action Task Force, and SOCA is a member of the Egmont Group. The UK cooperates with foreign law enforcement agencies investigating narcotics-related financial crimes. The Mutual Legal Assistance Treaty (MLAT) between the UK and the United States has been in force since 1996, and the two countries signed a reciprocal asset sharing agreement in March 2003. The UK also has an MLAT with the Bahamas. Additionally, there is a memorandum of understanding in force between U.S. Immigration and Customs Enforcement and HM Revenue and Customs.

The United Kingdom has a comprehensive anti-money laundering/counterterrorist financing (AML/CTF) regime. Authorities should continue to track and examine the effects of the SOCAP change regarding acts and assets in or from foreign jurisdictions, and revisit this legislation to determine whether it has been effective, or whether it has enabled exploitation. The UK should continue its active participation in international fora and its efforts to provide assistance to jurisdictions with nascent or developing AML/CTF regimes.

Uruguay

Uruguay is a money laundering country of primary concern. While the level of domestic money laundering and related crimes is considered relatively low, Uruguay's financial system nevertheless remains vulnerable to money laundering and terrorist financing risks associated with international sources that may be involved in Uruguay's cross-border financial operations. Officials from the Uruguayan police and judiciary assess that there is a growing presence of Mexican and Colombian cartels in the Southern Cone and fear they will begin operating in earnest in Uruguay. Drug dealers are slowly starting to participate in other illicit activities like car theft and trafficking in persons, according to the police. The Government of Uruguay (GOU) acknowledges that there is also a risk of money laundering in the real estate sector and in the sports industry, and seeks to develop new regulations soon to address this emerging vulnerability.

In the past, Uruguay's strict bank secrecy laws, liberal currency exchange and capital mobility regulations, and overall economic stability made it a regional financial center (mainly for Argentine depositors) vulnerable to money laundering, though the extent and the nature of suspicious financial transactions have been unclear. In recent years, however, Uruguay has made significant efforts to expand the reach and strength of its anti-money laundering and counterterrorist financing (AML/CTF) regime, including by enacting several laws to criminalize money laundering and terrorist financing. These recent developments have led to the prosecution of 25 individuals; new legislation and

enforcement efforts also resulted in the freezing of $1.5 million in assets, the detection of $1.7 million in undeclared cross-border cash and other financial instrument movements, and increases in suspicious activities reports and information requests about international financial activities.

One government owned commercial bank (which has roughly half of total deposits and credits), 14 foreign-owned banks, six financial houses, six offshore banks, and 21 representative offices of foreign banks comprise Uruguay's financial sector. The six offshore banks are subject to the same laws and regulations as local banks, with the GOU requiring them to be licensed through a formal process that includes a background investigation. Offshore trusts are not allowed. Bearer shares may not be used in banks and institutions under the authority of the Central Bank, and any share transactions must be authorized by the Central Bank. The financial private sector, most of which is foreign-owned, has developed self-regulatory measures against money laundering, such as the Codes of Conduct approved by the Association of Banks and the Chamber of Financial Entities (1997), the Association of Exchange Houses (2001), and the Securities Market (2002).

There are twelve free trade zones located throughout the country. While most are dedicated almost exclusively to warehousing, three host a wide variety of tenants performing a wide range of services, including financial services. Two free trade zones were created exclusively for the development of the paper and pulp industry. Some of the warehouse-style free trade zones have been used as transit points for containers of counterfeit goods bound for Brazil and Paraguay. There are nine casinos, eight of which are government owned, and 26 premises with slot machines (although media reports indicate a problem with businesses running unregistered slot machines). Four of the eight government-owned casinos are run by the state, and the other four by private sector concessions. Fiduciary companies called SAFIs (Anonymous Societies for Financial Investment) are also thought to be a convenient conduit for illegal money transactions. As of January 1, 2006, all SAFIs were required to provide the names of their directors to the Finance Ministry. In addition, the GOU implemented a comprehensive tax reform law in July 2007, which prohibited the establishment of new SAFIs as of that date. All existing SAFIs are to be eliminated by 2010. The tax reform law also implemented a personal income tax for the first time in Uruguay.

Uruguay achieved several notable actions against financial crime in 2008. Parliament passed laws 18.362 and 18.390 in October 2008, which created three courts and two prosecutor's offices dedicated to prosecuting organized crime. These new offices will deal with money laundering, terrorism financing, banking fraud, tax fraud, counterfeiting, as well as drug trafficking, corruption, trafficking of weapons, child prostitution, among other crimes.

In the past several years, 25 individuals were prosecuted for money laundering; 22 were related to drugs and three to sexual exploitation. Uruguay's first arrest and prosecution for money laundering (under Law 17.835) occurred in October 2005 and resulted in the conviction of the offender. In another ongoing high-profile case, 14 people were indicted in September 2006 for a money laundering charge tied to the largest cocaine seizure in Uruguay's history; in June 2008, the kingpin was convicted. This case has significantly invigorated the GOU's efforts to fight money laundering and to push for increased reporting of suspicious activities. Other cases involving another large cocaine seizure and proceeds from trafficking in 2007 and undeclared transit of gold from Brazil in 2008 are also under investigation. There have been no reported cases or investigations related to terrorist financing.

Unlike neighboring Argentina and Brazil, tax evasion is not an offense in Uruguay, which in practice limits cooperation possibilities because the local Financial Intelligence Unit's Financial Information and Analysis Unit (UIAF) cannot share tax-related information with its counterparts. Nevertheless, the UIAF is becoming increasingly active in cooperation with counterpart financial units and judiciaries from other countries. From 2006 to 2008, the number of information requests received by the UIAF rose from 25 to 50 (mainly from Argentina and Brazil), and the number of information requests issued

by the UIAF rose from five to 16. Information requests received by the UIAF from the judiciary also rose from 10 to 26 in the same period.

In Uruguay, money laundering is treated as an autonomous criminal offense, separate from the underlying crimes, which extends, under certain circumstances, to offenses committed in other countries. Money laundering is criminalized under Law 17.343 of 2001 and Law 17.835 of 2004. The courts have the power to seize and confiscate property, products or financial instruments linked to money laundering activities. Law 17.343 identifies money laundering predicate offenses to include narcotics trafficking; corruption; terrorism; smuggling (valued more than $20,000); illegal trafficking in weapons, explosives and ammunition; trafficking in human organs, tissues, and medications; trafficking in human beings; extortion; kidnapping; bribery; trafficking in nuclear and toxic substances; and illegal trafficking in animals or antiques.

Four government bodies are responsible for coordinating GOU efforts to combat money laundering: (1) the UIAF, (2) the National Anti-Drug Secretariat, (3) the Coordination Commission for Anti-Money Laundering and Terrorism Financing, and (4) the National Internal Audit. Decree 245/007 (passed July 2008), transformed the Center for Training on Money Laundering (CECPLA) into the Coordination Commission for Anti-Money Laundering and Terrorism Financing. The Commission works under the National Anti-Drug Secretariat, which is the senior authority for anti-money laundering policy and is headed by the President's Deputy Chief of Staff. The Commission's board is composed of government entities involved in anti-money laundering efforts: the head of the UIAF and the Ministries of Education (via prosecutors), of the Interior (via the police force), Defense (via the Naval Prefecture), and Economy and Finance. The Director of the Commission serves as coordinator for all government entities involved and sets general policy guidelines. The Director defines and implements GOU policies, in coordination with the Finance Ministry and the UIAF. The UIAF is responsible for supervising all financial institutions and the National Internal Audit Office (AIN) is responsible for overseeing all nonfinancial institutions, such as casinos and real estate firms.

The UIAF is a directorate of the Central Bank and is structured in three units: information and analysis, exchange houses, and money laundering control. GOU and private sector entities cannot refuse to provide information to the UIAF on the grounds of banking, professional or tax secrecies. Law 17.835 expands the realm of entities required to file Suspicious Activity Reports (SARs), making reporting of such suspicious financial activities a legal obligation, and conferring upon the UIAF the authority to request additional related information.

Law 18.401 (from October 2008) placed the UIAF under the Central Bank's Superintendent of Financial Services, and tasked it with several new activities that enhance its power as a mechanism to stop money laundering. While severely understaffed in the past, the UIAF achieved its goal in 2008 of establishing a staff of 19 people. Through funding from the Organization of American States (OAS), the UIAF is updating its hardware and software systems in order to receive SARs electronically, develop electronic early-alarm systems for SARs, and improve control and analysis of its lists. The project is part of the Central Bank's strategic plan and is expected to be finished this year.

The UIAF has circulated to financial institutions the list of individuals and entities included in UN 1267 Sanctions Committee and published it on its web page. It also works with lists from the Department of Treasury's Office of Foreign Assets Control (OFAC) and the European Union and is exploring options to purchase commercial databases with global blacklists. The UIAF is also working on a Politically Exposed Persons (PEPs) list that will also be published on their website.

Law 17.835 significantly strengthens the GOU's anti-money laundering regime by including specific provisions related to the financing of terrorism and to the freezing of assets linked to terrorist organizations, as well as provisions for undercover operations and controlled deliveries. Under this law, terrorist financing is a separate, autonomous offense that can be prosecuted from other terrorism-related crimes. The law, however, suffers from a narrow definition, which is limited to the financing of

terrorists or terrorist organizations where specific terrorist acts have been committed or are being planned. As a result, the law does not specifically cover the provision or collection of funds by known terrorists or terrorist organizations for purposes other than terrorist acts. Beyond criminalizing terrorist financing, Law 17.835 provides the courts with the power to seize and confiscate property, products or financial instruments linked to money laundering activities. Despite this power, the way real estate is registered complicates efforts to track money laundering in this sector, especially in the partially foreign-owned tourist sector. The UIAF and other government agencies must obtain a judicial order to have access to the name of titleholders. The GOU is in the process of implementing a national computerized registry that will facilitate the UIAF's access to titleholders' names. As of November 2008, the project is at an advanced stage of implementation and its completion target date is December 2008. The UIAF is already using the loaded data for investigation purposes. In 2007, the UIAF froze assets for 72 hours in three occasions, for a total of $1.5 million.

Under Law 17.835, all obligated entities must implement anti-money laundering policies, such as thoroughly identifying customers, recording transactions more than $10,000 in internal databases, and reporting suspicious transactions to the UIAF. This obligation extends to all financial intermediaries, including banks, currency exchange houses, stockbrokers, insurance companies, casinos, art dealers, and real estate and fiduciary companies. Law 17.835 also extended reporting requirements to all persons entering or exiting Uruguay with more than $10,000 in cash or in monetary instruments. This measure has resulted in the detection of over $1.7 million in about 20 undeclared cross-border movements since the declaration requirement entered into force in December 2006. The GOU imposes a fine of 30 percent on all undeclared funds. Since all movements were detected at one single customs office, and given Uruguay's porous borders, the GOU suspects that many more movements are passing undetected. Lawyers, accountants, and other nonbanking professionals that habitually carry out financial transactions or manage commercial companies on behalf of third parties are also required to identify customers whose transactions exceed $15,000 and report suspicious activities of any amount.

Implementing regulations have been issued by the Central Bank for all entities it supervises (banks, currency exchange houses, stockbrokers, and insurance companies), and are being issued by the Ministry of Economy and Finance for all other reporting entities. On November 26, 2007, the Central Bank issued Circular 1.978, which requires financial intermediary institutions, exchange houses, credit administration companies and correspondent financial institutions to implement detailed anti-money laundering and counterterrorist financing policies. This circular mandates financial intermediaries to report conversion of foreign exchange or precious metals over $10,000 into bank checks, deposits or other liquid instruments; conversion of foreign exchange or precious metals over $10,000 into cash; cash withdrawals over $10,000; and wire transfers over $ 1,000. As of November 2008, the Central Bank's Capital Market Division is considering requesting reports of transactions with securities over $10,000. Circular 1.978 requires these institutions to pay special attention to business with PEPs; persons, companies, and financial institutions from countries that are not members of the Financial Action Task Force (FATF) or a FATF-style regional body; and persons, companies, and financial institutions from countries that are subject to FATF special measures for failure to comply with the FATF Recommendations.

Obligated entities are mandated to know their customers on a permanent basis, keep adequate records and report suspicious activities to the UIAF. Compliance by reporting entities increased from 94 SARs in all of 2006 to 174 SARs in 2007 and 152 in the first half of 2008. SARs are largely concentrated within the financial system, with banks accounting for 70 percent of total reports and exchange houses for the remaining 30 percent. Other obligated entities, like casinos or real estate agents, have issued few SARs. Sixteen cases from SARs have been filed before the Judiciary but none have been prosecuted. The recent high profile money laundering cases have provided a boost to the money laundering issue and the Central Bank's efforts.

The GOU states that safeguarding the financial sector from money laundering is a priority, and Uruguay remains active in international anti-money laundering efforts. Uruguay is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. The GOU is also a member of the OAS Inter-American Drug Abuse Control Commission (CICAD) Experts Group to Control Money Laundering. Uruguay and the United States are parties to a mutual legal assistance treaty that entered into force in 1994. Uruguay is also a founding member of the Financial Action Task Force for South America (GAFISUD). Since early 2005, the former director of the GOU's Center for Training on Money Laundering Issues (CECPLA) has served as GAFISUD Executive Secretary, and has offered the services of Uruguay's anti-money laundering training center to GAFISUD.

Several notable developments that will strengthen Uruguay's anti-money laundering regime are expected in 2009. As of November 2008, the GOU has been working on legislation that would incorporate new money laundering predicate offenses to include prostitution, child pornography, intellectual property, trademark offenses, misappropriation, fraudulent bankruptcy, and counterfeiting of notes. Such legislation is also expected to identify new obligated entities that will be subject to Uruguay's anti-money laundering regime. New types of financial entities, including firms that provide services of leasing and custody of safety boxes, professional trust funds, professional advisors on investments, transportation of assets and wiring services, will be supervised by the UIAF. Various nonfinancial entities, including notaries, auctioneers, free zone exploiters, real estate brokers and other real estate intermediaries, will be supervised by the AIN.

The 2008 rendering of accounts (Law 18.362) granted the AIN additional funding of about $1 million for staffing needs, but the agency would need further leverage to achieve its new tasks. Pending legislation also provides for new investigation techniques (such as undercover and collaborator agents), new witness protection systems, and new measures to facilitate and speed up the seizure of assets. The UIAF plans to submit its application for Egmont Group membership, which is being sponsored by Brazil, in 2009. The GOU will await parliamentary approval of the impending legislation before applying, since that draft legislation incorporates the possibility of exchanging information to fight terrorism financing, which had been involuntarily left out of previous provisions.

The GOU has taken significant steps over the past few years to strengthen its anti-money laundering and counterterrorist financing regime. To continue its recent progress, Uruguay should expedite the passage of pending legislation and continue its implementation and enforcement of recently enacted legislation. The GOU's UIAF should prioritize efforts to gain membership in the Egmont Group; such a step would enable it to share financial information with other FIUs globally. The GOU should exert greater vigilance in detecting undeclared and cross-border movements of cash and other monetary instruments, as well as enhanced regulating and monitoring of its real estate sector and sports industries.

Uzbekistan

Uzbekistan is not an important regional financial center and does not have a well-developed financial system. Corruption, narcotics trafficking and smuggling generate the majority of illicit proceeds. Local and regional drug-trafficking and other organized crime organizations control narcotics proceeds and proceeds from other criminal activities, such as smuggling of cash, high-value transferable assets (e.g., gold), property, or automobiles. Drug traffickers and other organized crime groups also control illicit proceeds in foreign bank accounts. Uzbekistan is home to a significant black market for smuggled goods. Since the GOU imposed a very restrictive trade and import regime in the summer of 2002, smuggling of consumer goods, already a considerable problem, increased dramatically. Recent laws

and Presidential Decrees suspending Uzbekistan's anti-money laundering regime have caused concern among the international community.

Many Uzbek citizens continue to make a living by illegally shuttle-trading goods from neighboring countries and regions, including China, Turkey, Iran, India, Korea, the Middle East, Europe, and the U.S. The black market for smuggled goods does not appear to be significantly funded by narcotics proceeds, but, as noted above, drug dealers use the robust black market to clean their drug-related money.

Legitimate business owners, ordinary citizens, and foreign residents generally attempt to avoid using the Uzbek banking system for transactions except when absolutely required, because of the onerous nature of the Government of Uzbekistan's (GOU) financial control system, fear of GOU seizure of assets, and lack of trust in the banking system as a whole. The Central Bank of Uzbekistan (CBU), General Prosecutor's Office (GPO), and the National Security Service (NSS) closely monitor all domestic banking transactions for tax and currency control purposes. As a result, Uzbek citizens have functioning bank accounts only if they are required to do so by law. They only deposit funds that they are legally required to deposit, and often resort to subterfuge to avoid depositing currency. In particular, banks are required to know, record, and report the identity of customers engaging in significant transactions, including the recording of large currency transactions above $40,000. All transactions involving sums greater than U.S. $1,000 in salary expenses for legal entities and U.S. $500 in salaries for individuals must be tracked and reported to the authorities. The CBU unofficially requires commercial banks to report on private transfers to foreign banks exceeding U.S. $10,000. The Central Bank of Uzbekistan (CBU) states that deposits from individuals have been increasing in recent years, but it is still seeking to increase consumer confidence in banks.

Reportedly, the unofficial, unmonitored cash-based market creates an opportunity for small-scale terrorist or drug-related laundering activity destined for internal operations. For the most part, the funds generated by smuggling and corruption are not directly laundered through the banking system, but through seemingly legitimate businesses, such as restaurants and high-end retail stores. There appears to be virtually no money laundering through formal financial institutions in Uzbekistan because of the extremely high degree of supervision and control over all bank accounts in the country exercised by the Central Bank, Ministry of Finance, General Prosecutor's Office (GPO), the National Security Service (NSS), and state-owned and controlled banks. Although Uzbek financial institutions are not known to engage in illegal transactions in U.S. currency, illegal unofficial exchange houses, where the majority of cash-only money laundering takes place, deal in Uzbek soum and U.S. dollars. Moreover, drug dealers and others can transport their criminal proceeds in cash across Uzbekistan's porous borders for deposit in the banking systems of other countries, such as Kazakhstan, Russia or the United Arab Emirates.

Money laundering from the proceeds from drug-trafficking and other criminal activities is a criminal offense. Article 41 of the Law on Narcotic Drugs and Psychotropic Substances (1999) stipulates that any institution may be closed for performing a financial transaction for the purpose of legalizing (laundering) proceeds derived from illicit narcotics trafficking. GOU officials noted that there have been no related cases thus far in Uzbekistan. The law protects reporting individuals with respect to their cooperation with law enforcement entities. The GOU has reportedly not adopted laws holding individual bankers responsible if their institutions launder money.

The Law on Banks and Bank Activity (1996), article 38, stipulates conditions under which banking information can be released to law enforcement, investigative and tax authorities, prosecutor's office and courts. Different conditions for disclosure apply to different types of clients—individuals and institutions. In September 2003, Uzbekistan enacted a bank secrecy law that prevents the disclosure of client and ownership information for domestic and offshore financial services companies to bank supervisors and law enforcement authorities. In all cases, banks can disclose private information to

prosecution and investigation authorities if a criminal investigation is underway. They can provide information to the courts on the basis of a written request in relation to cases currently under consideration. Tax authorities can also obtain protected banking information in cases involving the taxation of a bank's client. GOU officials noted that the secrecy law does not apply if a group is on a list of designated terrorist organizations.

Penalties for money laundering are from ten to fifteen years imprisonment, under Article 243 of the Criminal Code. This article defines the act of money laundering to include as punishable acts the transfer; conversion; exchange; or concealment of origin, true nature, source, location, disposition, movement and rights with respect to the assets derived from criminal activity.

The Department of Investigation of Economic Crimes within the Ministry of Internal Affairs (MVD) conducts investigations of all types of economic offenses. A specialized structure within the NSS and the Department on Tax, Currency Crimes and Legalization of Criminal Proceeds is also authorized to conduct investigations of money laundering offenses. Unofficial information from numerous law enforcement officials indicates that there have been few, if any, prosecutions for money laundering under article 243 of the Criminal Code since its enactment in 2001. Officials from the Office of the State Prosecutor reported that there were 11 money laundering-related cases in 2006 and five in 2007. As of October 2008, officials stated that three of the sixteen cases are still pending. The status or disposition of the other cases is unknown. Overall, the GOU reportedly lacks a sufficient number of experienced and knowledgeable agents to investigate money laundering. Moreover, although the law has been in effect for more than five years, officials from the State Prosecutor's Office reported that Article 243 does not work well because different judges and attorneys can interpret it in different ways.

In 2004, Uzbekistan enacted a basic AML/CTF regime that contained a range of AML/CTF provisions, including CDD, record keeping, reporting, and the establishment of an FIU. While the AML/CTF law went into effect on January 1, 2006, important parts of the law were repealed pursuant to several presidential decrees and an additional law. In particular, provisions relating to suspicious transaction reporting, CDD, information gathering, and the FIU were suspended until 1 January 2013. In addition, pursuant to a February 2008 decree that expires on 1 April 2009, banks are prohibited from inquiring into customers' source of funds and providing customer information to any government authorities.

Specifically, the Presidential Decrees had the effect of rescinding the main legislative provisions as follows: Presidential Decree No. PP-565 of 12 January 2007 suspended the obligation of covered entities to report to the FIU information about threshold financial transactions (i.e., cash transactions above U.S. $40,000 (approximately), and suspicious transactions), and further subjects such reports to legislation on bank secrecy. Presidential Decree No. PP-586 of 20 February 2007 suspended all AML/CTF Presidential and Cabinet of Ministers Decrees until 1 January 2013. It rescinds the various authorities provided to the FIU including the authority to establish a financial intelligence system, monitor financial and property transactions, identify money laundering and terrorist financing mechanisms and channels, share information on identified crimes with law enforcement agencies for criminal prosecution, cooperate and exchange information with foreign agencies and international organizations on AML/CTF issues based on international obligations and agreements of Uzbekistan. Presidential Decree No. PP-586 also suspends the Cabinet of Ministers Regulations on the creation of the FIU database and the reporting procedure. Law RU-94 of 27 April 2007 suspends Articles 9 and 13-16 of the main AML/CTF Law which correspond to these FIU authorities and include all of the covered entities' obligations regarding customer identification/due diligence, threshold transaction reports, suspicious transaction reports and internal control requirements. However, Article 21 on record keeping remains in place.

Separately and in addition, on 20 February 2008, the Government of Uzbekistan issued Decree No. YP-3968 that expires on 1 April 2009. This decree imposes blanket bank secrecy within the Uzbek financial system for natural persons—residents of Uzbekistan. It prohibits financial institutions from requesting background information from customers making deposits and transferring money from abroad into Uzbek banks; and further prohibits financial institutions from providing such information with respect to those customers to any governmental authorities. The express purpose of this decree—as stated in its preamble—is to reinforce people's confidence in the banking system, reduce the volume of cash transactions that are not made through banks, and create "further incentives to attract people's idle funds to deposits with commercial banks as a key source of investment resources for rapid development of the country's economy."

Together, the above actions had a marked effect: banks reported 17,000 suspicious transactions in a six-month period before the law was suspended, compared with 400 in the six months following the law's suspension.

These executive and legislative actions led the FATF ICRG to review the AML/CTF situation in Uzbekistan. The FATF Plenary has issued two public statement (February 2008 and October 2008), expressing FATF's concerns about Uzbekistan's AML/CTF vulnerabilities; calling upon Uzbekistan to restore its AML/CTF regime and establish an AML/CTF regime that meets international standards; and calling on its members and urging all jurisdictions to advise their financial institutions to take the risk arising from the deficiencies in Uzbekistan's AML/CTF regime into account for enhanced due diligence. A joint FATF-EAG High-Level/Technical Mission to Uzbekistan took place on November 24-25, 2008, which gathered information on Uzbekistan's AML/CTF deficiencies, measures currently in place, and steps taken to address FATF's concerns. During the course of this mission, the GOU acknowledged that it is currently relying on a tax regulatory system to partially compensate for their repealed AML/CTF provisions, but that these measures are inadequate and that an actual AML/CTF regime needs to be restored. The Uzbek authorities further acknowledged that FATF's concerns were reasonable and committed to instituting an AML/CTF regime that meets international standards by enacting necessary legislation within 6 months that will address FATF's concerns.

Existing controls on transportation of currency across borders would, in theory, facilitate detection of the international transportation of illegal source currency. When entering or exiting the country, foreigners and Uzbek citizens are required to report all currency they are carrying. Residents and nonresidents may bring the equivalent of U.S. $10,000 into the country tax-free, and authorities assess a one-percent duty on amounts in excess of this limit. Customs officers at Tashkent Airport vigorously enforce this limit and target foreign nationals for careful searches as they depart the country. Those caught in possession of more currency than they declared upon entering Uzbekistan are assessed severe fines and may face criminal charges. Residents may export up to the equivalent of U.S. $2,000. Residents wishing to take out higher amounts must obtain authorization to do so; amounts over U.S. $2,000 must be approved by an authorized commercial bank, and amounts over U.S. $5,000 must be approved by the CBU. International cash transfers to or from an individual person are limited to U.S. $5,000 per transaction; there is no monetary limit on international cash transfers made by legal entities, such as a corporation. However, Uzbekistan does not permit direct wire transfers to or from other Central Asian countries; a third country must be used.

Uzbekistan permits offices of international business companies, which are subject to the same regulations as domestic businesses, but prohibits offshore banks. Other forms of exempt or shell companies are not officially present.

Article 155 of Uzbekistan's Criminal Code and the law "On Fighting Terrorism" criminalize terrorist financing. The latter law names the NSS, the MVD, the Committee on the Protection of State Borders, the State Customs Committee, the Ministry of Defense, and the Ministry for Emergency Situations as responsible for implementing the counterterrorist legislation, and designates the NSS as the

coordinator for government agencies fighting terrorism. The GOU has the authority to identify, freeze, and seize terrorist assets. Uzbekistan has circulated to its financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list. In addition, the GOU has circulated the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224 to the CBU, which has, in turn, forwarded these lists to banks operating in Uzbekistan. According to the CBU and the Office of the State Prosecutor, no assets have been frozen.

Other than a plan to step up enforcement of currency regulations, the GOU has taken no steps to regulate alternative remittance systems such as hawala, or deter black market exchanges, trade-based money laundering, or the misuse of gold, precious metals and gems. GOU officials noted that most overseas migrants work in more advanced countries, such as Russia or Korea, where financial institutions track remittances. Although officially there is complete currency convertibility, in reality, authorities can significantly delay or outright refuse the conversion, and do so during such times as the annual autumn cotton harvest, when cash supplies are needed internally to support the extensive mobilization of people and machinery to collect the crop. Foreign companies complain that they must wait over six months to convert the profits from local sales into foreign currencies in order to transfer the money out of Uzbekistan.

The GOU closely monitors the activities of charitable and nonprofit entities, such as NGOs, that terrorism financiers could exploit. In February 2004, the Cabinet of Ministers issued Decree 56 to allow the government to vet grants to local NGOs from foreign sources, ostensibly to fight money laundering and terrorist financing. Given the high level of supervision of charities and other nonprofits, and the perceived threat from the Islamic Movement of Uzbekistan (IMU) and other extremist organizations, it is unlikely that the NSS would knowingly allow any funds to be funneled to terrorists through Uzbekistan-based charitable organizations or NGOs.

Uzbekistan has established systems for identifying, tracing, freezing, seizing, and forfeiting proceeds of both narcotics-related and money laundering-related crimes. Current laws include the ability to seize items used in the commission of crimes, such as conveyances used to transport narcotics, farm facilities (except land) where illicit crops are grown or which are used to support terrorist activity, legitimate businesses if related to criminal proceeds and bank accounts. The banking community, which is entirely state-controlled and with few exceptions, state-owned, cooperates with efforts to trace funds and seize bank accounts. Uzbek law does not allow for civil asset forfeiture, but the Criminal Procedure Code provides for "civil" proceedings within a criminal case to decide forfeiture issues. As a practical matter, authorities conduct these proceedings as part of the criminal case. The obstacles to enacting such laws are largely rooted in the widespread corruption that exists within the country.

In 2000, Uzbekistan established a special fund to direct confiscated assets to law enforcement activities. In 2004, the Cabinet of Ministers closed the Special Fund. Under the new procedure, each agency manages the assets it seizes. There is also a specialized fund within the MVD to reward those officers who directly participate in or contribute to law enforcement efforts leading to the confiscation of property. This fund has generated 20 percent of its assets from the sale of property confiscated from persons who have committed offenses, such as the organization of criminal associations, bribery and racketeering. The GOU is believed to enforce existing drug-related asset seizure and forfeiture laws enthusiastically, although there is no information regarding the total dollar value of crime related assets. Reportedly, existing legislation does not permit sharing of seized narcotics assets with other governments.

The GOU realizes the importance of international cooperation in the fight against drugs and transnational organized crime and has made some efforts to integrate the country into the system of international cooperation. Uzbekistan has entered into bilateral agreements for cooperation or

exchange of information on drug related issues with the United States, Germany, Italy, Latvia, Bulgaria, Poland, China, Iran, Pakistan, the Commonwealth of Independent States (CIS), and all the countries in Central Asia. It has multilateral agreements under the framework of the CIS and the Shanghai Cooperation Organization, and under memoranda of understanding.

Uzbekistan signed an "Agreement on Narcotics Control and Law Enforcement Assistance" with the United States on August 14, 2001, with two supplemental agreements that came into force in 2004. Uzbekistan does not have a Mutual Legal Assistance Treaty with the United States. However, Uzbekistan and the United States have reached informal agreement on mechanisms for exchanging adequate records in connection with investigations and proceedings relating to narcotics, terrorism, terrorist financing and other serious crimes. In the past, Uzbekistan has cooperated with appropriate law enforcement agencies of the USG and other governments investigating financial crimes and several important terrorist-related cases. Cooperation in these areas became increasingly problematic in an atmosphere of strained U.S.-Uzbekistan bilateral relations, but there was gradual improvement in 2008.

Uzbekistan has been a member of the Eurasian Group on Combating Money Laundering and the Financing of Terrorism (EAG), a FATF-style regional body, since 2005.

The GOU is an active party to the relevant agreements concluded under the CIS, the Central Asian Economic Community (CAEC), the Economic Cooperation Organization (ECO), and the Shanghai Cooperation Organization. Uzbekistan is a party to the 1988 UN Drug Convention, the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption.

A lack of trained personnel, resources, and modern equipment continues to hinder Uzbekistan's efforts to fight money laundering and terrorist financing. Moreover, the decrees suspending the main provisions of the money laundering law until 2013 and the February 2008 Presidential decree providing an amnesty on deposits were major AML/CTF setbacks. The GOU should immediately rescind these decrees while continuing to refine its legislation to bring it into conformity with international standards. Additional revisions should expand the cross-border currency reporting rules to cover the transfer of monetary instruments, precious metals and stones. Regulatory and law enforcement agencies should have access to financial institution records, so that they can properly conduct compliance examinations and investigations. While the 2006 establishment of an FIU was a positive step, the repeal of the AML/CTF provisions makes it impossible for the Uzbek FIU to function effectively. Assuming restoration of Uzbekistan's AML/CTF regime, much will depend on the FIU's ability to become fully operational and to cooperate effectively with other GOU law enforcement and regulatory agencies in receiving and disseminating information on suspicious transactions.

Vanuatu

Vanuatu's offshore sector is vulnerable to money laundering, as Vanuatu has historically maintained strict bank secrecy provisions that have the effect of preventing law enforcement agencies from identifying the beneficial owners of offshore entities registered in the sector. Due to allegations of money laundering, and in response to pressure from the Financial Action Task Force (FATF), a few United States-based banks announced in December 1999 that they would no longer process U.S. dollar transactions to or from Vanuatu. The Government of Vanuatu (GOV) responded to these concerns by introducing reforms designed to strengthen domestic and offshore financial regulation. The GOV passed amendments to four of its main pieces of legislation relative to money laundering and terrorist financing during its last session of Parliament in November 2005. The four pieces of legislation affected are the Mutual Assistance in Criminal Matters Act No. 31 of 2005, the Financial Transaction Reporting Act No. 28 of 2005, the Counter-Terrorism and Transnational Organized Crime Act No. 29

of 2005, and the Proceeds of Crime Act (Amendment) Act No. 30 of 2005. The International Companies Act was amended in 2006. Taken with Ministerial Order No. 15 (April 2007), this amendment immobilized Bearer Shares and required the identification of Bearer Share custodians.

Vanuatu's financial sector includes five domestic licensed banks (that carry out domestic and offshore business); one credit union; eight international banks; seventy insurance companies (both life and general); and eight foreign exchange instrument dealers, money remittance dealers and bureaux de change, all of which are regulated by the Reserve Bank of Vanuatu. Since the passage of the International Banking Act of 2002, the Reserve Bank of Vanuatu (RBV) regulates the offshore banking sector that includes the eight international banks and approximately 3,603 international business companies (IBCs), as well as offshore trusts and captive insurance companies. These institutions were once regulated by the Financial Services Commission. IBCs are now registered with the Vanuatu Financial Services Commission (VFSC). This change was one of many recommendations of the 2002 International Monetary Fund Module II Assessment Report (IMFR) that found Vanuatu's onshore and offshore sectors to be "noncompliant" with many international standards.

Regulatory agencies in Vanuatu have instituted stricter procedures for issuance of offshore banking licenses under the International Banking Act No. 4 of 2002, and continue to review the status of previously issued licenses. All financial institutions, both domestic and offshore, are required to report suspicious transactions and to maintain records of all transactions for six years, including the identities of the parties involved.

The Financial Transaction Reporting Act (FTRA) of 2000 established the Vanuatu Financial Intelligence Unit (VFIU) within the State Law Office. Under the Financial Transactions Reporting (Amendment) Act No. 28 of 2005 (FTRAA), the VFIU has a role in ensuring compliance by financial services sector with financial reporting obligations. The VFIU receives suspicious transaction reports (STRs) filed by banks and distributes them to the Public Prosecutor's Office, the Reserve Bank of Vanuatu, the Vanuatu Police Force, the Vanuatu Financial Services Commission, and law enforcement agencies or supervisory bodies outside Vanuatu. The VFIU also issues guidelines to, and provides training programs for, financial institutions regarding record keeping for transactions and reporting obligations. The Act also regulates how such information can be shared with law enforcement agencies investigating financial crimes. Financial institutions within Vanuatu must establish and maintain internal procedures to combat financial crime. Every financial institution is required to keep records of all transactions. Five key pieces of information are required to be kept for every financial transaction: the nature of the transaction, the amount of the transaction, the currency in which it was denominated, the date the transaction was conducted, and the parties to the transaction. As of July 2007, the FIU had received a total of 33 suspicious transaction reports. Vanuatu has no AML/CTF prosecutions and conviction, to date.

Although the amendments have been withdrawn from Parliament twice, the FTRA amendments were finally passed in November 2005 and enacted in late February 2006. The amendments include mandatory customer identification requirements; broaden the range of covered institutions required to file STRs to include auditors, trust companies, and company service providers; and provide safe harbor for both individuals and institutions required to file STRs. In addition to STR filings, financial institutions will now be required to file currency transaction reports (CTRs) that involve any single transaction in excess of Vanuatu currency Vatu (VT) 1,000,000, or its equivalent in a foreign currency, and wire transfers into and out of Vanuatu in excess of VT 1,000,000 ($9,100). The amendments also require financial institutions to maintain internal procedures to implement reporting requirements, appoint compliance officers, establish an audit function to test their anti-money laundering and counterterrorist financing procedures and systems, as well as provide the VFIU a copy of their internal procedures. Failure to do so will result in a fine or imprisonment for an individual, or a fine in the case of a corporate entity. The amendments supersede any inconsistent banking or other secrecy provisions and clarify the VFIU's investigative powers.

The amended FTRA defines financial institutions to include casinos licensed under the Casino Control Act No.6 of 1993, lawyers, notaries, accountants and trust and company service providers. The scope of the legislation is so broad that entities such as car dealers and various financial services that currently do not exist in Vanuatu (and are unlikely to in the future) are covered. Applications by foreigners to open casinos are subject to clearance by the Vanuatu Investment Promotion Authority (VIPA) which reviews applications and conducts a form of due diligence on the applicant before issuing a certification to the Department of Customs and Inland Revenue to issue an appropriate license. The Department of Customs and Inland Revenue receives applications from local applicants directly. In June 2008, the FIU began to conduct on-site reviews of money exchanges, law firms, accounting firms, real estates companies and casinos. The onsite examination is a part of the VFIU's awareness campaign to familiarize these industries to their obligations, set forth under the FTRAA.

The Vanuatu Police Department and the VFIU are the primary agencies responsible for ensuring money laundering and terrorist financing offences are properly investigated in Vanuatu. The Public Prosecutions Office (PPO) is responsible for the prosecution of money laundering and terrorist financing offences. The Vanuatu Police Department has established a Transnational Crime Unit (TCU), and is responsible for investigations involving money laundering and terrorist financing offences, the identification and seizure of criminal proceeds, as well as conducting investigations in cooperation with foreign jurisdictions.

Supervision of the financial services sector is divided between three main agencies: the Reserve Bank of Vanuatu (RBV), the Vanuatu Financial Services Commission (VFSC) and the Customs and Revenue Branch of the Ministry of Finance. The RBV is responsible for supervising and regulating domestic and offshore banks. The VFSC supervises insurance providers, credit unions, charities and trust and company service providers, but is unable to issue comprehensive guidelines or to regulate the financial sectors for which it has responsibility.

The Serious Offenses (Confiscation of Proceeds) Act 1989 criminalized the laundering of proceeds from all serious crimes and provided for seizure of criminal assets and confiscation after a conviction. The Proceeds of Crime Act (2002) retained the criminalization of the laundering of proceeds from all serious crimes, criminalized the financing of terrorism, and included full asset forfeiture, restraining, monitoring, and production powers regarding assets. The Proceeds of Crime Act No. 30 of 2005 through its new Section 74A effective in November 2005 required all incoming and outgoing passengers to and from Vanuatu to declare to the Department of Customs cash exceeding one million VT in possession ($9,100).

Vanuatu passed the Mutual Assistance in Criminal Matters Act in December 2002 for the purpose of facilitating the provision of international assistance in criminal matters for the taking of evidence, search and seizure proceedings, forfeiture or confiscation of property, and restraints on dealings in property that may be subject to forfeiture or seizure. The Attorney General possesses the authority to grant requests for assistance, and may require government agencies to assist in the collection of information pursuant to the request. The Extradition Act of 2002 includes money laundering within the scope of extraditable offenses.

The amended International Banking Act has now placed Vanuatu's international and offshore banks under the supervision of the Reserve Bank of Vanuatu. Section 5(5) of the Act states that if existing licensees wish to carry on international banking business after December 31, 2003, the licensee should have submitted an application to the Reserve Bank of Vanuatu under Section 6 of the Act for a license to carry on international banking business. If an unregistered licensee continued to conduct international banking business after December 31, 2003, in violation of Section 4 of the Act, the licensee is subject to a fine or imprisonment. Under Section 19 of the Act, the Reserve Bank can conduct investigations where it suspects that an unlicensed person or entity is carrying on international

banking business. Since this time, three international banking businesses have had their licenses revoked.

One of the most significant requirements of the amended legislation is the banning of shell banks. As of January 1, 2004, all offshore banks registered in Vanuatu must have a physical presence in Vanuatu, and management, directors, and employees must be in residence. At the September 2003 plenary session of the Asia/Pacific Group on Money Laundering (APG), Vanuatu noted its intention to draft new legislation regarding trust companies and company service providers. The VFSC has prepared the Trust and Company Services Providers Bill and the GOV will present the bill before Parliament during the first half of 2008. The new legislation will cover disclosure of information with other regulatory authorities, capital and solvency requirements, and "fit and proper" requirements. In 2005, Vanuatu enacted Insurance Act No. 54, drafted in compliance with standards set by the International Association of Insurance Supervisors. Insurance Regulation Order No.16 of 2006 was issued on May 2006, and regulates the insurance industry, to include intermediary and agents roles.

International Business Companies (IBC) traditionally could be registered using bearer shares, shielding the identity and assets of beneficial owners of these entities. Secrecy provisions protected all information regarding IBCs and provided penal sanctions for unauthorized disclosure of information. These secrecy provisions, along with the ease and low cost of incorporation, made IBCs ideal mechanisms for money laundering and other financial crimes. Section 125 of the International Companies Act No. 31 of 1992 (ICA), provided a strict secrecy provision for information disclosure related to shareholders, beneficial ownership, and the management and affairs of IBCs registered in Vanuatu. This provision, in the past, has been used by the industry to decline requests made by the VFIU for information. However, section 17(3) of the new amended FTRA clearly states that the new secrecy-overriding provision in the FTRA overrides section 125 of the ICA. Moreover, the International Companies (Amendment) Act No. 45 of 2006 (ICA) revised the regime governing IBC operations. Ministerial Order No. 15 of 2007 created a Guideline of Custody of Bearer Shares, which immobilized Bearer Shares and requires the identification of Bearer Share custodians.

In November 2005, Vanuatu passed the Counter-Terrorism and Transnational Organized Crime Act (CTTOCA) No. 29 of 2005. The CTTOCA was brought into force on 24 February 2006. The aim of the Act is to implement UN Security Council Resolutions and Conventions dealing with terrorism and transnational organized crime, to prevent terrorists from operating in Vanuatu or receiving assistance through financial resources available to support the activities of terrorist organizations, and to criminalize human trafficking and smuggling. Terrorist financing is criminalized under section 6 of the CTTOCA. Section 7 of the CTTOCA makes it an offence to "directly or indirectly, knowingly make available property or financial or other related services to, or for the benefit of, a terrorist group." The penalty upon conviction is a term of imprisonment of not more than 25 years or a fine of not more than VT 125 million (U.S. $1,000,000), or both. Section 8 criminalizes dealing with terrorist property. The penalty upon conviction is a term of imprisonment of not more than 20 years or a fine of not more than VT 100 million (U.S. $876,500), or both. There were no terrorist financing or terrorism-related prosecutions or investigations in 2006.

In March 2006, the APG conducted a mutual evaluation of Vanuatu, the results of which were reported at the APG plenary meeting in November 2006. The APG evaluation team found that Vanuatu had improved its anti-money laundering and counterterrorist financing regime since its first evaluation in 2000 by criminalizing terrorist financing, requiring a wider range of entities to report to the VFIU and enhancing supervisory oversight of obligated entities. However, some deficiencies remain: the GOV has not taken a risk-based approach to combating money laundering and terrorist financing; a person who commits a predicate offense for money laundering cannot also be charged with money laundering; and current law does not require the names and addresses of directors and shareholders to be provided upon registration of an IBC. It is further recommended that the GOV issue regulations under the FTRAA, particularly those relating to customer due diligence. The GOV was

advised to issue guidelines to financial institutions and DNFBPs, with regard to customer identification, record keeping, reporting obligations, identification of suspicious transactions and money laundering and financing of terrorism typologies.

The GOV has created the Vanuatu Financial Sector Assessment Group (VFSAG). The VFSAG is comprised of the Director-General of the Prime Minister's Office, the Director-General of Finance, the Attorney-General, the Governor and Deputy Governor of the RBV, the Commissioner of the Vanuatu Financial Services Commission (VFSC), Department of Finance and a member of the VFIU. The VFSAG have discussed the possibility of creating an additional working group that will be responsible for the implementation of recommendations and policies relating to Vanuatu's AML/CTF regime. The proposed group will be comprised of law enforcement officials, legal entities, and the VFIU.

In addition to its membership the Asia Pacific Group on Money Laundering, Vanuatu is a member of the Offshore Group of Banking Supervisors, the Commonwealth Secretariat, and the Pacific Island Forum. Its Financial Intelligence Unit became a member of the Egmont Group in June 2002. Vanuatu is a party to the UN Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime and the 1988 UN Drug Convention. Vanuatu is not a party to the UN Convention against Corruption. The VFIU has a memorandum of understanding with Australia.

The Government of Vanuatu should implement all the provisions of its Proceeds of Crime Act and enact all additional legislation that is necessary to bring both its onshore and offshore financial sectors into compliance with international standards. The GOV should also establish a viable asset forfeiture regime and circulate the updated UNSCR 1267 Sanctions Committee updated list of designated terrorist entities. With the passage of the amendments to the FTRAA, the GOV should continue to initiate outreach to all reporting institutions regarding new CDD obligations, as well as establish legislative requirements for financial institutions to have policies and procedures to address risks arising from new or developing technologies and non-face-to-face businesses in particular internet accounts. Vanuatu should become a party to the UN Convention against Corruption.

Venezuela

Venezuela is not a regional financial center, nor does it have an offshore financial sector. The relatively small but modern banking sector, which consists of 60 banks, primarily serves the domestic market. However, Venezuela is a country of primary money laundering concern and one of the principal drug-transit countries in the Western Hemisphere. Venezuela's proximity to drug producing countries, weaknesses in its anti-money laundering regime, refusal to cooperate with the United States in mutual legal assistance matters, including on counternarcotics activities, and rampant corruption throughout the law enforcement, judicial, banking, and banking regulatory sectors continue to make Venezuela vulnerable to money laundering. The main sources of money laundering are from proceeds generated by cocaine and heroin trafficking organizations, the embezzlement of funds from the petroleum industry and illegal currency exchange on the black market. Trade-based money laundering, such as the Black Market Peso Exchange, through which money launderers furnish narcotics-generated dollars in the United States to commercial smugglers, travel agents, investors, and others in exchange for Colombian pesos, remains a prominent method for laundering narcotics proceeds. There has been an increase in money laundering due to a lack of access to foreign currency exchange and diminished investment opportunities. Transparency International's Corruption Perception Index for 2008 ranks Venezuela at 158 of 180 countries on the index.

Venezuelan law provides for the establishment of free trade ports and zones in any part of the country, as designated by the Executive. Currently, Venezuela has four free trade zones: Paraguana Peninsula, Margarita Island, Merida and Santa Elena de Uairen. Merida's free trade privileges extend solely to cultural items or scientific or technological development. The Law on Free Trade Zones designates

that the customs authority of each jurisdiction is responsible for its respective free trade zone. The Ministry of Economy and Finance is responsible for the oversight of the customs authority with regard to free trade zones. It is reported that many black market traders ship their wares through Margarita Island's free trade zone. Reportedly, some money is also laundered through the real estate market in Margarita Island. However, statistics regarding activities in the free trade zones were not available as of the time of this report.

The 2005 Organic Law against Organized Crime criminalized money laundering as an autonomous offense, punishable by a sentence of eight to 12 years in prison and a fine equivalent to the increased value obtained by the crime. Those who cannot establish the legitimacy of possessed or transferred funds, or are aware of the illegitimate origins of those funds, can be charged with money laundering, without any connection to drug trafficking. In addition to establishing money laundering as an autonomous offense, the Organic Law against Organized Crime broadens asset forfeiture and sharing provisions, adds conspiracy as a criminal offense, strengthens due diligence requirements, and provides law enforcement with stronger investigative powers by authorizing the use of modern investigative techniques, such as the use of undercover agents. The Organic Law against Organized Crime addresses bank secrecy, requiring supervised entities to report suspicious activities. Supervised entities may not invoke bank secrecy to avoid reporting. Contravention of the law based upon the notion of bank secrecy is punishable by a fine of $84,000 to $126,000. The Organic Law against Organized Crime coupled with the Law against the Trafficking and Consumption of Narcotics and Psychotropic Substances, effectively brings Venezuela's Penal Code in line with the 1988 UN Drug Convention.

Under the Organic Law Against Organized Crime, terrorist financing is a crime against public order in Venezuela and is criminalized to the extent that if an individual finances, belongs to, acts or collaborates with armed bands or criminal groups with the purpose to wreak havoc, catastrophes, fires, explosions of mines, bombs or other explosive devices or to subvert the constitutional order and democratic institutions or gravely alter the public peace. Punishment for these activities is a prison term of ten to 15 years. Terrorist financing, however, is not adequately criminalized in accordance with the Financial Action Task Force (FATF) Nine Special Recommendations on Terrorist Financing. The law does not establish terrorist financing as a separate crime, nor does it provide adequate mechanisms for freezing assets.

In spite of the advances made with the passage of the Organic Law against Organized Crime in 2005, there is little evidence that the Government of Venezuela (GOV) has the political will to effectively enforce the legislation it has promulgated. To date, not a single case has been tried under the law. Reportedly, many, if not most, judicial and law enforcement officials remain ignorant of the Law against Organized Crime and its specific provisions, and the GOV's financial intelligence unit (FIU) does not have the necessary autonomy to operate effectively. Widespread corruption within the judicial and law enforcement sectors also undermines the effectiveness of the law as a tool to combat the growing problem of money laundering.

The Superintendent of Banks and Other Financial Institutions (SBOIF) is the entity that supervises and examines supervised financial institutions for compliance with anti-money laundering laws and regulations. The SBOIF conducts audits of supervised financial institutions, including a review of anti-money laundering compliance procedures, on a yearly cycle with the possibility of off-cycle audits on an as-needed basis.

Under the Organic Law against Organized Crime and Resolution 185.01 of the SBOIF anti-money laundering controls have been implemented, requiring strict customer identification requirements and the reporting of both currency transactions over a designated threshold and suspicious transactions. These controls apply to all banks (commercial, investment, mortgage, and private), insurance and reinsurance companies, savings and loan institutions, financial rental agencies, currency exchange

houses, money remitters, money market funds, capitalization companies, frontier foreign currency dealers, casinos, real estate agents, construction companies, car dealerships, hotels and the tourism industry, travel agents, and dealers in precious metals and stones. These entities, with the exception of the insurance industry and designated nonfinancial businesses and professions, are required to file suspicious and cash transaction reports with Venezuela's FIU, the Unidad Nacional de Inteligencia Financiera (UNIF). Financial institutions are required to maintain records for a period of five years.

The UNIF was created under the SBOIF in July 1997 and began operating in June 1998. The UNIF is not an autonomous entity. The UNIF has a staff of approximately 30 and has undergone multiple bureaucratic changes, with six different directors presiding over the UNIF since 2004. The UNIF receives reports on currency transactions (CTRs) exceeding approximately $10,000 and suspicious transaction reports (STRs) from institutions regulated by the SBOIF: the National Securities and Exchange Commission, the Central Bank of Venezuela and the Bank Deposits and Protection Guarantee Fund. The Venezuelan Association of Currency Exchange Houses (AVCC), which counts all but one of the country's money exchange companies among its membership, voluntarily complies with the same reporting standards as those required of banks. Some institutions regulated by the SBOIF, such as tax collection entities and public service payroll agencies, are exempt from the reporting requirement. The SBOIF also allows certain customers of financial institutions—those who demonstrate "habitual behavior" in the types and amounts of transactions they conduct—to be excluded from currency transaction reports filed with the UNIF. SBOIF Circular 3759 of 2003 requires financial institutions that fall under the supervision of the SBOIF to report suspicious activities related to terrorist financing.

In addition to STRs and CTRs, the UNIF also receives reports on the domestic transfer of foreign currency exceeding $10,000, the sale and purchase of foreign currency exceeding $10,000, and summaries of cash transactions that exceed approximately $2,100. The UNIF does not, however, receive reports on the physical transportation of currency or monetary instruments into or out of Venezuela. A system has been developed for electronic receipt of CTRs, but STRs must be filed in paper format. Obligated entities are forbidden to reveal reports filed with the UNIF or suspend accounts during an investigation without official approval, and are also subject to sanctions for failure to file reports with the UNIF. Article 67 of the Organic Law against Organized Crime protects individuals and institutions with regard to cooperation with law enforcement and the judicial process. However, this protection expires 15 days after the individual exits Venezuela.

The UNIF analyzes STRs and other reports, and refers those deemed appropriate for further investigation to the Public Ministry (the Office of the Attorney General). For the six month period ending in June 2008, the UNIF received 603 STRs. In 2007, the UNIF forwarded approximately 40 percent of the STRs it received to the Attorney General's Office. The Attorney General's office subsequently opens and oversees the criminal investigation. Although the UNIF does not receive statistics from the Office of the Attorney General at this time concerning the number of prosecutions for money laundering, the UNIF is working on the implementation of a database for tracking cases referred to the Attorney General's office for investigation. The UNIF maintains several memoranda of understanding (MOUs) with Venezuelan government institutions regarding the sharing of information. In addition, the UNIF is working on updating all circulars and guidance so that the 2005 law is incorporated into its rules and regulations.

Prior to the passage of the 2005 Organic Law against Organized Crime, there was no special prosecutorial unit for the prosecution of money laundering cases under the Attorney General's office, which is the only entity legally capable of initiating money laundering investigations. As a result of the limited resources and expertise of drug prosecutors who previously handled money laundering investigations, there have only been three money laundering convictions in Venezuela since 1993 and all of them were narcotics-related. The Organic Law against Organized Crime calls for a new unit to be established, the General Commission against Organized Crime, with specialized technical expertise

in the analysis and investigation of money laundering and other financial crimes. This commission has not been established to date. The Organic Law against Organized Crime also expanded Venezuela's mechanisms for freezing assets tied to illicit activities. A prosecutor may now solicit judicial permission to freeze or block accounts in the investigation of any crime included under the law. However, to date there have been no significant seizures of assets or successful money laundering prosecutions as a result of the law's passage. The SBOIF has distributed to its supervised financial entities the list of individuals and entities that have been included on the UN 1267 sanctions committee's consolidated list. No statistics are available on the amount of assets frozen, if any.

The UNIF has been a member of the Egmont Group since 1999 and has signed bilateral information exchange agreements with counterparts worldwide. The UNIF does share information with Egmont Group members, but does not publish statistical information regarding such information sharing. Due to the unauthorized disclosure of information provided by the Financial Crimes Enforcement Network, (FinCEN, the U.S. FIU) to the UNIF, FinCEN suspended information exchange with the UNIF in January 2007. FinCEN and the UNIF are currently negotiating the terms and necessary measures that need to be taken by the UNIF to guarantee the protection of FinCEN information before information exchange will resume between the two FIUs. Once this issue is resolved, FinCEN will begin sharing financial intelligence with the UNIF again.

Venezuela participates in the Organization of American States Inter-American Commission on Drug Abuse Control (OAS/CICAD) Money Laundering Experts Working Group and is a member of the Caribbean Financial Action Task Force (CFATF). The GOV is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention for the Suppression of the Financing of Terrorism. The GOV has signed, but not yet ratified, the UN Convention against Corruption. Although the GOV committed to sharing money laundering information with U.S. law enforcement authorities under the 1990 Agreement Regarding Cooperation in the Prevention and Control of Money Laundering Arising from Illicit Trafficking in Narcotics Drugs and Psychotropic Substances, which entered into force on January 1, 1991, no such information sharing occurred in 2008. Venezuela and the United States signed a Mutual Legal Assistance Treaty (MLAT) in 1997. Venezuela is currently undergoing a CFATF mutual evaluation, with a report to be presented at the May 2009 CFATF plenary. Its last evaluation was undertaken in 1999.

The GOV took no significant steps to expand its anti-money laundering regime in 2008. There were no prosecutions or convictions for money laundering in 2008, and this is unlikely to change in 2009. The 2005 passage of the Organic Law against Organized Crime was a step toward strengthening the GOV's abilities to fight money laundering. However, Venezuela needs to enforce the law by implementing the draft procedures to expedite asset freezing, establishing an autonomous financial investigative unit, and ensuring that law enforcement and prosecutors have the necessary expertise and resources to successfully investigate and prosecute money laundering cases. The GOV should also adequately criminalize the financing of terrorism and establish procedures for freezing terrorist assets in order to conform to international standards. The UNIF should continue to pursue the normalization of information exchange with FinCEN, and take the necessary steps to ensure that information exchanged with other FIUs is subject to the appropriate safeguards mandated by the Egmont Group. The GOV should honor its commitment to share information with U.S. law enforcement agencies.

Vietnam

Vietnam is not an important regional financial center, but is the site of significant money laundering activities. Vietnam remains a largely cash-based economy and both U.S. dollars and gold are widely used as a means of exchange and of stored value. Remittances are a large source of foreign exchange, exceeding annual disbursements of development assistance. Remittances from the proceeds of

narcotics in Canada and the United States are also a significant source of money laundering as are proceeds attributed to Vietnam's role as a transit country for narcotics.

The Vietnamese banking sector is in transition from a state-owned to a partially privatized industry. At present, approximately 50 percent of the assets of the banking system are held by state-owned commercial banks that allocate much of the available credit to state-owned enterprises. Almost all trade and investment receipts and expenditures are processed by the banking system, but neither trade nor investment transactions are monitored effectively. As a result, the banking system could be used for money laundering either through over or under invoicing exports or imports or through phony investment transactions. Official inward remittances for the first six months of 2008 are estimated to be approximately $3.5 billion. These amounts are generally transmitted by wire services and while officially recorded, there is no reliable information on either the source or the recipients of these funds. Financial industry experts believe that actual remittances may be double the official figures. There is evidence that large mounts of cash are hand carried into Vietnam, which is legal as long as the funds are declared. The Government of Vietnam (GOV) does not require any explanation of the source or intended use of funds brought into the country in this way. In 2006, Vietnam Airlines was implicated in a U.S. $93 million money laundering scheme uncovered by the Australian Crime Commission. Vietnamese organized crime syndicates operating in Australia and involved in money transfer businesses used the airline to help smuggle money to Vietnam.

A form of informal value transfer service, which often operates through the use of domestic jewelry and gold shops, is widely used to transfer funds within Vietnam. Money or value transmitters are defined as financial institutions by Decree No. 74 and are therefore subject to its AML-related provisions; however, the informal transmitters have not been brought under regulation or supervision.

The U.S. Drug Enforcement Agency (DEA) is engaged in a number of investigations targeting significant ecstasy and marijuana trafficking organizations, composed primarily of Vietnamese legal permanent residents in the United States and Vietnamese landed immigrants in Canada as well as naturalized U.S. and Canadian citizens. These drug trafficking networks are capable of laundering tens of millions of dollars per month back to Vietnam, exploiting U.S. financial institutions to wire or transfer money to Vietnamese bank and remittance accounts, as well as engaging in the smuggling of bulk amounts of U.S. currency and gold into Vietnam. The drug investigations have also identified multiple United States-based money remittances businesses that have remitted over $100 million annually to Vietnam. It is suspected that the vast amount of that money is derived from criminal activity. Law enforcement agencies in Australia and the United Kingdom have also tracked large transfers of drug profits back to Vietnam.

Articles 250 and 251 of the Amended Penal Code criminalize money laundering. Article 251 of the Penal Code defines the offense of legalizing money or property obtained through the commission of crime, while the Article 250 defines the offense of harboring (such as acquiring, possessing, hiding or concealing etc.) or consuming (such as trading, exchanging etc.) property obtained from the commission of crime by others. Although this offence aims at punishing those who generate a black market for consuming property acquired through the commission of crime rather than those who legalize the illicit origin of such property, its guilty acts cover some forms of money-laundering prescribed under the Palermo Convention. The Counter-Narcotics Law, which took effect June 1, 2001, makes two narrow references to money laundering in relation to drug offenses: it prohibits the "legalizing" (i.e., laundering) of monies and/or property acquired by committing drug offenses (article 3.5); and, it gives the Ministry of Public Security's specialized counternarcotics agency the authority to require disclosure of financial and banking records when there is a suspected violation of the law. The Penal Code governs money laundering related offenses but no money laundering cases have been prosecuted under Article 251 to date. Similarly, while there have been many convictions under Article 250, such convictions have not involved money laundering, but instead relate to harboring property from crimes of others. Article 251 does not meet current international standards; among other

weaknesses, the law requires a very high burden of proof (essentially, a confession) to pursue AML allegations, so prosecutions are non-existent and international cooperation is extremely difficult. The GOV presented a draft revision of Article 251 to the National Assembly in October 2008, for approval sometime in 2009.

In June 2005, the GOV issued Decree 74/2005/ND-CP on Prevention and Combating of Money Laundering. The Decree covers acts committed by individuals or organizations to legitimize money or property acquired from criminal activities. The Decree applies to banks and nonbank financial institutions. The State Bank of Vietnam (SBV) and the Ministry of Public Security (MPS) take primary responsibility for preventing and combating money laundering. Neither the Penal Code nor the Decree currently covers counterterrorist finance. A new draft article defining and criminalizing terrorism finance was presented to the National Assembly in October 2008 for approval sometime in 2009.

The SBV supervises and examines financial institutions for compliance with anti-money laundering/counterterrorist financing regulations. Financial institutions are responsible for knowing and recording the identity of their customers. They are required to report cash transactions conducted in one day with aggregate value of Vietnam Dong (VND) 200 million (approximately U.S. $13,000) or more, or equivalent amount in foreign currency or gold. The threshold for aggregate daily account based transactions is VND 500 million (approximately $31,000). Cash transaction reporting is not effective due to the absence of a suitable information technology solution to facilitate such reporting. Furthermore, financial institutions are required to report all suspicious transactions. Banks are also required to maintain records for seven years or more. Banks are responsible for keeping information on their customers secret, but they are required to provide necessary information to law enforcement agencies for investigation purposes.

Foreign currency (including notes, coins and traveler's checks) in excess of U.S. $7,000 and gold of more than 300 grams must be declared at customs upon arrival and departure. There is no limitation on either the export or import of U.S. dollars or other foreign currency provided that all currency in excess of $7,000 (or its equivalent in other foreign currencies) is declared upon arrival and departure, and supported by appropriate documentation. If excess cash is not declared, it is confiscated at the port of entry/exit and the passenger may be fined.

The 2005 Decree on Prevention and Combating of Money Laundering provides for provisional measures to be applied to prevent and combat money laundering. Those measures include 1) suspending transactions; 2) blocking accounts; 3) sealing or seizing property; 4) seizing violators of the law; and, 5) taking other preventive measures allowed under the law.

The 2005 Decree also provides for the establishment of an Anti-Money Laundering Information Center (AMLIC) under the State Bank of Vietnam (SBV). Similar to a Financial Intelligence Unit (FIU), the AMLIC functions as the sole body to receive and process financial information required by the Decree. It has the right to request concerned agencies to provide information and records for suspected transactions. The AMLIC was formally established and began operations since February 2006. The Director of the center is appointed by the Governor of the SBV and reports directly to the Governor on anti-money laundering issues. SBV acts as the sole agency responsible for negotiating, concluding and implementing international treaties and agreements on exchange of information on transactions related to money laundering. In December 2008, SBV signed an information sharing agreement with Interpol's Vietnam office.

The AMLIC has 23 full time staff members, including a Director and two Deputy Directors and is working to hire more staff. The FIU is organized into three divisions: Administrative and Research, Collecting and Analyzing Information; and, Technical and Network. The FIU has established liaison with ministries and agencies such as Ministries of Justice, Public Security, Finance, Foreign Affairs, the Supreme People's Procuracy, the Supreme People's Court, and the Banking Association. The

AMLIC has virtually no IT capacity and a very low level of analytical ability. In spite of these drawbacks, AMLIC has begun to conduct awareness training with local financial institutions and with the public, and has its own section on the SBV website

The AMLIC has received 37 suspicious transaction reports and has referred two STRs to MPS for investigation. The MPS is responsible for investigating money laundering related offences. There is no information from MPS on investigations, arrests, and prosecutions for money laundering or terrorist financing, but the SBV reports that there are two cases pending prosecution in 2008. MPS is responsible for negotiating and concluding international treaties on judicial assistance, cooperation and extradition in the prevention and combat of money laundering related offenses. MPS signed a nonbinding Memorandum of Understanding with DEA in 2006 to strengthen law enforcement cooperation in combating transnational drug-related crimes, including money laundering, but claims it is unable to provide such information due to constraints within the Vietnamese legal system.

In 2007 Vietnam became a member of the Asia/Pacific Group on Money Laundering (APG). As a member of APG, Vietnam underwent a mutual evaluation of its AML/CTF regime in November, 2008. The results of the review will be discussed at the annual APG meeting in July, 2009. The Prime Minister has also ordered the formation of an inter-agency anti-money laundering coordination committee, to be chaired by a Deputy Prime Minister.

Vietnam is a party to the UN Convention for the Suppression of the Financing of Terrorism. Reportedly, Vietnam plans to draft new legislation governing counterterrorist financing, though it will not set a specific time frame for this drafting. Currently SBV circulates to its financial institutions the list of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list. No related assets have been identified.

Vietnam is a party to the 1988 UN Drug Convention. Under existing Vietnamese legislation, there are provisions for seizing assets linked to drug trafficking. In the course of its drug investigations, MPS has seized vehicles, property and cash, though the seizures are usually directly linked to drug crimes. Final confiscation requires a court finding. Reportedly, MPS can notify a bank that an account is "seized" and that is sufficient to have the account frozen.

The GOV should promulgate all necessary regulations to implement fully the 2005 Decree on the Prevention and Combating of Money Laundering. Vietnam should also enact legislation to fully criminalize money laundering and to make terrorist financing a criminal offense, as well as including provisions to address the prevention and suppression of terrorist financing. Vietnam should ratify the UN Conventions against Transnational Organized Crime and Corruption. Vietnamese law enforcement authorities should investigate money laundering, trade fraud, alternative remittance systems, and other financial crimes in Vietnam's shadow economy. The AMLIC should be equipped with an electronic information reporting system to enable it to effectively collect, store and analyze financial transactions. Vietnam should continue to take those additional steps necessary to establish its anti-money laundering/counterterrorist financing regime so that it comports with international standards.

Yemen

The financial system in Yemen is not well developed and the extent of money laundering is not known. Yemen is not considered a regional financial center. Financial institutions are subject to regulations and limited monitoring by the Central Bank of Yemen (CBY). However, alternative remittance systems, such as hawala, are not subject to scrutiny and are vulnerable to money laundering and other financial abuses—including possible terrorist financing. The official banking sector is relatively small with 17 commercial banks, including four Islamic banks. Yemeni banks account for

approximately 60 percent of total banking activities. All banks are under the supervision of the CBY. Yemen has no offshore banks or shell companies.

Yemen has a large underground economy due, in part, to the profitability of the smuggling of trade goods and contraband. Khat is a recreational drug produced from the leaves of a bush grown in parts of East Africa and Arabia. The use of khat is common in Yemen and there have been a number of investigations over the years of khat being smuggled from Yemen and East Africa into the United States with profits laundered and repatriated via hawala networks. Smuggling and piracy are rampant along Yemen's sea border with Oman, across the Red Sea from the Horn of Africa, and along the land border with Saudi Arabia in the North.

In April 2003 Yemen's Parliament passed anti-money laundering (AML) legislation (Law 35). The legislation criminalizes money laundering for a wide range of crimes, including narcotics offenses, kidnapping, embezzlement, bribery, fraud, tax evasion, illegal arms trading, and monetary theft, and imposes penalties of three to five years of imprisonment. Yemen has no specific legislation criminalizing terrorist financing nor are there obligations to report suspicious transactions associated with terrorist financing. In November 2007 the Cabinet sent a draft of more comprehensive anti-money laundering and counterterrorist financing legislation to Parliament to accommodate international standards. However, it appears unlikely the bill will be passed in the near term.

Law 35 requires banks, financial institutions, and precious metals and gems dealers to verify the identity of individuals and entities that open accounts to keep records of transactions for up to five years, and to report and file suspicious transaction reports (STRs). In addition, the law requires that reports be submitted to the Anti-Money Laundering Information Unit (AMLIU), which acts as the country's financial intelligence unit (FIU). The AMLIU reports to the Anti-Money Laundering Committee (AMLC).

The AMLC, housed within the CBY, is composed of representatives from the Ministries of Finance, Foreign Affairs, Justice, Interior, and Industry and Trade, the Central Accounting Office, the General Union of Chambers of Commerce and Industry, the Association of Banks, and the CBY. The AMLC is authorized to issue regulations and guidelines and provide training related to combating money laundering and other financial crimes. Law 35 grants the AMLC the ability to exchange information with foreign entities that have signed a letter of understanding with Yemen; however the FIU is not autonomous since it is not granted the authority to receive information from other competent authorities without referring to AMLC or the CBY Governor.

There are approximately 448 registered money exchange businesses in Yemen, which serve primarily as currency exchangers in addition to performing funds transfer services. Money transfer businesses are required to register with Central Bank, and can open offices at multiple locations. Fund transfers that exceed the equivalent of $10,000 require permission from the CBY. The CBY has not performed examination of the money exchange business for anti-money laundering and combating the finance of terrorism (AML/CTF) compliance.

The AMLIU has only a few employees. The AMLIU uses the services of field inspectors from the CBY's Banking Supervision Department for some of the FIU duties. The AMLIU has no database and is not networked to other government data systems. The CBY provides training to other members of the government to assist in elements of anti-money laundering enforcement. In September 2008, the World Bank initiated a restructuring project which will establish divisions within the AMLIU dealing with the receipt of STRs, financial investigations, database maintenance and the exchange of information. The project also aims at increasing the number of AMLIU staff to 15. The functions of the AMLIU are restricted to money laundering issues and do not cover terrorist financing.

The head of the AMLC is empowered by law to ask local judicial authorities to enforce foreign court verdicts based on reciprocity. There is no Mutual Legal Assistance Treaty (MLAT) or extradition

treaty between Yemen and the United States. The Legal Attaché's Office at the U.S. Embassy in Sana'a routinely passes requests for information and assistance to the Government of Yemen (GOY) concerning terrorist financing and other issues but seldom receives responses.

Prior to passage of the AML law, the CBY issued Circular 22008 in April 2002, instructing financial institutions to positively identify the place of residence of all persons and businesses that establish relationships with them. The circular also requires that banks verify the identity of persons or entities that wish to transfer more than the equivalent of $10,000, when they have no accounts at the banks in question. The same provision applies to beneficiaries of such transfers. The circular also prohibits inbound and out-bound money transfer of more than the equivalent of $10,000 cash without prior permission from the CBY, although this requirement is not strictly enforced. The circular is distributed to the banks along with a copy of the Basel Committee's "Customer Due Diligence for Banks," concerning "know your customer" procedures and "Core Principles for Effective Banking Supervision." However, the due diligence process is limited in most financial institutions, particularly the nonbanking ones, to customer identification. Little attention is paid to account activities or the size of the account. The existing AML law protects individuals, banks and others with respect to their cooperation with law enforcement entities. The CBY has a program to educate the public and the financial sector about the proper ways of detecting and reporting suspicious financial transactions. Since 2005, only ten STRs have been filed with the AMLIU, with a few forwarded to the Office of the Public Prosecutor for suspected money laundering. There has not been any money laundering prosecutions or convictions in Yemen.

Yemen has no cross-border cash declarations or disclosure requirements. Customs inspectors do file currency declaration forms if funds are discovered. Yemen has one free trade zone (FTZ) in the port city of Aden. Identification requirements with the FTZs are enforced. For example, truckers must file the necessary paperwork in relevant trucking company offices and must wear ID badges. FTZ employees must undergo background checks by police, the Customs Authority and employers. There is no evidence that the FTZ is being used for trade-based money laundering or terrorist financing schemes.

In September 2003, the CBY responded to the UNSCR 1267 Sanctions Committee's consolidated list, the Specially Designated Global Terrorists by the United States pursuant to E.O. 13224, and Yemen's Council of Ministers' directives, by issuing circulars 75304 and 75305 to all banks operating in Yemen. Circulars 75304 and 75305 directed banks to freeze the accounts of 144 persons, companies, and organizations, and to report any findings to the CBY. As a result, one account was immediately frozen. In 2006, the CBY began issuing a circular every three months containing an updated list of persons and entities belonging to Al-Qaida and the Taliban. However, since the February 2004 addition of Yemeni Sheikh Abdul Majid Zindani to the UNSCR 1267 Sanctions Committee's consolidated list, the Yemeni government has made no known attempt to enforce the sanctions and freeze his assets. There is no information on whether Yemeni authorities have identified, frozen, seized, or forfeited other assets related to terrorist financing.

The GOY has a forfeiture system in place. A judge must order the forfeiture for the items involved in or proceeds from the crime for which the defendant was convicted. Forfeiture is available for all crimes and extends to funds and property. Authorities deposit forfeited funds into the general treasury unless the funds are the proceeds from a drug offense, in which case the proceeds go to law enforcement authorities, who can use the proceeds to buy vehicles or other equipment. If the court orders a defendant to forfeit property, the judge issues an order to auction off the property to the public, with the funds from the auction going into the general treasury. In some instances, the courts can order real property, such as a dwelling, to be closed for one year before the owner may use it again. Yemen has not yet forfeited any real property.

In 2001 the government enacted a law governing charitable organizations. This law entrusts the Ministry of Social Affairs and Labor (MOSAL) with overseeing their activities. The law also imposes penalties of fines and/or imprisonment on any society or its members convicted of carrying out activities or spending funds for other than the stated purpose for which the society in question was established. In addition to keeping accounts under continuous supervision in coordination with the MOSAL, Central Bank Circular No. 33989 of June 2002 and Circular No. 91737 of November 2004, ordered banks to enhance controls regulating opening and managing charities' accounts.

Yemen is a member of the Middle East and North Africa Financial Action Task Force (MENAFATF). In 2007 there was a MENAFATF mutual evaluation of Yemen. The report has not been released. The United States concluded in a recent Financial Systems Assessment Team (FSAT) report that Yemen is in the early stages of developing its ability to control money laundering and numerous factors should be considered in developing programs to deal with the cash-intensive nature of the economy, significant levels of corruption, and problems in the judicial system.

In September 2008, the Yemeni President ordered the establishment of an independent supervisory committee, chaired by the Minister of Finance, which would meet on an ad-hoc basis, to oversee the government's anti-money laundering program and eventually appoint a technical committee to carry out the recommendations of the FSAT and MENAFATF recommendations.

Yemen is a party to the 1988 UN Drug Convention; it has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. The GOY is a party to the UN Convention against Corruption. Yemen is listed 141 out of 180 countries in Transparency International's 2008 Corruption Perception Index.

The Government of Yemen should continue to develop an anti-money laundering regime that adheres to international standards. Banks and nonbank financial institutions should enhance their capacity to detect and report suspicious financial transactions to the FIU, including those related to terror finance. The AMLIU needs substantial improvement of its operational capacity to enhance its analytical capabilities and other duties. Yemen should investigate the abuse of alternative remittance systems such as hawala networks with regard to money laundering and terrorist financing. Law enforcement and customs authorities should also examine trade-based money laundering and customs fraud. Yemen should enact specific legislation with respect to terrorist financing and forfeiture of the assets of those suspected of terrorism. Yemen should enforce sanctions and freeze the assets of Sheikh Abdul Majid Zindani, who was added to the UN 1267 Sanctions Committee's consolidated list in February 2004. Yemen should ratify the UN Convention against Transnational Organized Crime and should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism. Yemen has no institutionalized coordination for terrorism matters among the different ministries and has yet to implement steps listed under the UN international terrorism protocols, to which Yemen is a party.

Zimbabwe

Zimbabwe is not a regional financial center, but continued rapid economic deterioration has led to the growth of money laundering opportunities for regime officials and well-connected elites. This situation results from official corruption and impunity; a flourishing parallel exchange market; rampant smuggling of precious minerals; widespread evasion of exchange controls; and company ownership through nominees. Deficiencies in the Government of Zimbabwe's (GOZ) regulatory and enforcement framework contribute to Zimbabwe's potential as a money laundering destination. These deficiencies include an understaffed bank supervisory authority; a lack of trained regulators and investigators to investigate and enforce penalties for violations and financial crime; financial institutions determined to bypass the regulatory framework; limited asset seizure authority; a laissez-faire attitude toward compliance with the law on the part of elements of the business community;

ready acceptance of the U.S. dollar in transactions; and significant exports and illegal trading, particularly regarding gold and diamonds.

In July 2008, the GOZ implemented a currency re-denomination program that slashed ten zeros from Zimbabwe's currency (so that Z$10,000,000,000 became Z$1). The purpose of the campaign was to ease bookkeeping and the handling of cash transactions under runaway inflation and at the same time assert greater GOZ control over the financial sector.

In October 2008, the GOZ froze the majority of electronic bank transfers by suspending the Real-Time Gross Settlement system (RTGS). Reserve Bank of Zimbabwe (RBZ) officials were trying to curb a scheme known as "burning" in which people used RTGS transfers to evade the daily cash withdrawal limit. The RTGS transfers electronically moved funds in local currency from a single account into dozens of different accounts. From these accounts, runners extract the funds as cash withdrawals up to the daily cash withdrawal limit (raised to $500,000 Zimbabwean dollars in November 2008 (approximately $8.25). The scheme was profitable because the scarcity of cash had driven the value of the Zimbabwean dollar high above the value of electronic funds. The RBZ justified this radical step by stating it would curb money laundering and illegal foreign currency dealings on the parallel market. In November 2008, the RBZ reversed the unpopular suspension and reinstated the RTGS, stressing the need for banks to know their customers.

In 2008, the government also amended the schedule of fines applicable to those convicted of financial crimes. The new guidelines establish only minimum penalties, allowing judges to apply whatever maximum fine they determine appropriate to the offense. This is a means of curbing the hyperinflationary effect that makes worthless nearly any fine not immediately collected.

In December 2003, the GOZ enacted the Anti-Money Laundering and Proceeds of Crime Act. This bill criminalizes money laundering and implements a six-year record keeping requirement. In 2004, the GOZ adopted the more expansive Bank Use Promotion and Suppression of Money Laundering Act (the 2004 Act) that extends the anti-money laundering law to all serious offenses. The 2004 Act mandates a prison sentence of up to fifteen years for a conviction. It also criminalizes terrorist financing and authorizes the tracking and seizure of assets. The 2004 Act has reportedly raised human rights concerns due to the GOZ's history of selective use of the legal system against its political opponents, but its use to date has not been associated with any reported due process abuses or provoked any serious public opposition. The Exchange Control Order, enacted in 1996, obligates banks to require individuals who deposit foreign currency into a foreign currency account to submit a written disclosure of the sources of the funds.

The RBZ is the lead agency for prosecuting money laundering offenses. In May 2006, the RBZ issued new Anti-Money Laundering Guidelines that outline and reinforce requirements established in the Act for financial institutions and designated nonfinancial businesses and professions. These binding requirements address politically exposed persons, mandating obliged entities to gather and make available to regulators more personal data on these high-profile clients. Financial institutions must now keep records of accounts and transactions for at least ten years, and report any suspicious transactions to the financial intelligence unit (FIU). The Act also criminalizes tipping off. Failure to report suspected money laundering activities or violating rules on properly maintaining customer data carries a possible fine of Zimbabwe $3 million—a nearly worthless amount at current exchange rates—for each day that a financial institution is in default of compliance.

The 2004 Act provides for the establishment of Zimbabwe's FIU, housed within the RBZ and known as the Financial Intelligence Inspectorate and Evaluation Unit (FIIE). The FIIE receives suspicious transaction reports (STRs), issues guidelines (including the Anti-Money Laundering Guidelines issued in May 2006), and enforces compliance with procedures and reporting standards for obliged entities.

In June 2007, the RBZ installed an electronic surveillance system to track all financial transactions in the banking system. The FIIE reported that after the launch of the new system, there was a noticeable improvement in self-regulation at banks as demonstrated by an increase in the number of STRs received. During the year, the RBZ continued to tightly control limits on daily cash withdrawals for individuals and companies, ostensibly in an effort to curtail money laundering, but more likely to inhibit private sector parallel foreign exchange activities. When requested, the local banking community has cooperated with the GOZ in the enforcement of asset tracking laws. However, increasingly burdensome GOZ regulations and the resulting hostile business climate have led to growing circumvention of the law by otherwise legitimate businesses. In May, the RBZ cancelled the foreign currency exchange license of NMB Bank, the first indigenous bank in Zimbabwe, after a senior NMB official allegedly externalized more than $4.5 million in embezzled funds and fled the country. RBZ cited a breach of Exchange Control Regulations and a failure to report suspicious transactions as required under the Act.

The GOZ continued to arrest prominent Zimbabweans for activities that it calls "financial crimes." Prosecutions for such crimes, however, have reportedly been selective and politically motivated. The government often targets persons who have either fallen out of favor with the ruling party, or individuals without high-level political backing. Most financial crimes involved violations of currency restrictions that criminalize the externalization of foreign exchange. In light of the inability of the vast majority of businesses to access foreign exchange from the RBZ, most companies privately admit to externalizing their foreign exchange earnings or to accessing foreign currency on the parallel market. Moreover, the GOZ itself, through the RBZ, has been a major purchaser of foreign currency on the parallel market.

The 2001 Serious Offenses (Confiscation of Profits) Act establishes a protocol for asset forfeiture. The Attorney General may request confiscation of illicit assets. The Attorney General must apply to the court that has rendered the conviction within six months of the conviction date. The court can then issue a forfeiture order against any property. Despite the early date of this law compared to the money laundering legislation that followed, this law does define and incorporate money laundering among the bases for the GOZ to confiscate assets.

With the country in steep economic decline and increasingly isolated, Zimbabwe's laws and regulations remained ineffective in combating money laundering. The government's anti-money laundering efforts throughout the year appeared to be directed less to ensuring compliance than to securing the government's access to foreign currency, targeting opponents, and tightening control over precious minerals. Despite having the legal framework in place to combat money laundering, the sharp contraction of the economy, growing vulnerability of the population, and decline of judicial independence raise concerns about the capacity and integrity of Zimbabwean law enforcement. Transparency International ranks the Government of Zimbabwe at 166 of 180 countries on its 2008 Corruption Perceptions Index. The banking community and the RBZ have cooperated with the United States in global efforts to identify individuals and organizations associated with terrorist financing.

Zimbabwe is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Crime. Zimbabwe is also a party to the UN Convention against Corruption. It has not signed the UN Convention for the Suppression of the Financing of Terrorism. Zimbabwe joined the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) in 2003 and assumed the Presidency for ESAAMLG for the 2006/2007 administrative year. Zimbabwe experienced the first completed mutual evaluation undertaken by ESAAMLG. The report was adopted at the plenary and Council of Ministers meeting in August 2007.

The GOZ leadership should work to develop and maintain transparency, prevent corruption, and subscribe to practices ensuring the rule of law. The GOZ must also work toward reducing the rate of inflation, halting the economic collapse, and rebuilding the economy to restore confidence in the

currency. The GOZ can illustrate its commitment to combating money laundering and terrorist financing by using its legislation for the purposes for which it was designed, instead of using it to persecute opponents of the regime and nongovernmental organizations with which it disagrees. Once these basic prerequisites are met, the GOZ should endeavor to develop and implement an anti-money laundering/counterterrorist financing regime that comports with international standards. The GOZ should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism.