could help provide funds available for Colombia's anti-money laundering and counterterrorist financing regime.

Comoros

The Union of the Comoros (Comoros) consists of three islands: Grande Comore, Anjouan and Moheli. An ongoing struggle for influence continues between the Union and island presidents. Comoros is not a principal financial center for the region. An anti-money laundering (AML) law, which addresses many of the primary AML issues of concern, was passed by Presidential Decree in 2004. However, Comoran authorities lack the capacity to effectively implement and enforce the legislation, especially on the island of Anjouan. In May 2006, Muslim cleric Ahmed Abdallah Mohamed Sambi was elected President in the first peaceful change of power in Comoros' post-independence history. He won the election with 58 percent of the vote after campaigning on promises to fight corruption and unemployment. The presidency of the union rotates between the three islands. The former incumbent, Azali Assoumani, represented Grand Comore; Sambi is from Anjouan. The three islands in the Comoros continue to retain much of their autonomy, particularly with respect to their security services, economies, and banking sectors.

The 2004 federal-level AML law is based on the French model. The main features of the law are that it: 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 Comorian francs 5 million (approximately $12,500); and, criminalizes the provision of material support to terrorists and terrorist organizations. Although there is a suspicious activity filing requirement in the Union's AML law, there does not appear to be an independent financial intelligence unit in either Anjouan or the Union. As of February 2006, no suspicious transaction reports had been filed with the Comorian Central Bank in Grand Comore as required under the existing Union law, and the branch of the Central Bank located in Anjouan had no knowledge of the shell bank entities that have been licensed by Anjouan's Offshore Finance Authority, which apparently operates independently from the Union's Central Bank and has licenced some 300 offshore banks, many of which appear to be shell banks.

Foreign remittances from Comorans abroad in France, Mayotte (claimed by France) and elsewhere remain the most important influx of funds for most Comorons. Until recently most remittances came via informal channels, but in 2006 Western Union established a presence to capture part of this market.

Union authorities have limited ability to implement AML laws in Anjouan and Moheli. 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 some serious shortcomings and authorities lack the resources and expertise to enforce its provisions. For example, there is no absolute requirement to report large cash transactions. 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) but reportedly the law applies to Anjouan and not to the offshore entities it licenses. 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.

Union President Azali made efforts during his time as President to bring AML enforcement under Union government jurisdiction. In May 2005, he issued a note to the Ministry of Finance, the islands' presidents, and the Public Prosecution Department urging these institutions to take action with regard to any illegal offshore banking practices. The note indicated that all banking and financial institutions operating within the jurisdiction of the Union of the Comoros, whether offshore or onshore, must abide by the provisions of legislation No. 80-7 of May 3, 1980. According to article 7 of this legislation, a bank or any other financial institution cannot operate in the Union of the Comoros without prior authorization from the Union Finance Minister upon recommendation from the Comoros Central Bank. Thus, offshore banks operating in the autonomous islands of the Union of the Comoros without prior authorization from the Finance Minister contravene the May 3, 1980 legislation. Consequently, Azali's note directed the ministries and other government institutions responsible for banking and financial matters to take (or to see to it that the necessary measures are taken) to put an end to this "blatant illegality which is prejudicial to the Union of the Comoros." Also in May 2005, President Azali told the USG that the Comoran government is prepared to bring to justice the beneficiaries of illegal offshore licenses and sought the assistance and support of the USG in this endeavor. Since taking office, President Sambi has sought to have corrupt former officials prosecuted. A grossly inadequate budget, dysfunctional ministries, and a nonfunctioning judiciary limit Sambi. Throughout 2006 there were reports that Sambi's authority in Anjouan is limited. There are reports that high-ranking Comoran officials tolerate and possibly benefit from money laundering. The lack of political will is exacerbated by the lack of capacity.

While the Comoros is not a principal financial center for the region, Moheli and Anjouan may have attempted or may be attempting to develop an offshore financial services sector as a means to finance government expenditures. The Anjouan island government's claim that unrelated companies are presenting themselves as licensed by the government of Anjouan makes authoritative information on Anjouan's offshore sector difficult to establish. Both Moheli, pursuant to the International Bank Act of 2001, and Anjouan, pursuant to the Regulation of Banks and Comparable Establishments of 1999, license off-shore banks. Together, the islands have licensed more than 100 banks. Applicants for banking licenses in either jurisdiction are not required to appear in person to obtain their licenses. In Anjouan, 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) are required to obtain an offshore license and fax copies of these documents are acceptable. Even if additional information was to be required, it is doubtful that either jurisdiction has the ability or resources to authenticate and verify the information. Neither jurisdiction is capable, in terms of expertise or resources, of effectively regulating an offshore banking center. Anjouan, and probably Moheli as well, has delegated much of its authority to operate and regulate the offshore business to private, non-Comoran domiciled parties. In November 2004 and again in December 2005, Anjouan island government officials denied island government involvement in the offshore sector. They said the Union of the Comoros Central Bank was the only authority for the offshore banking sector in the country and insisted the Anjouan island government had not established its own central bank. They admitted that several years earlier the government of Anjouan considered starting an offshore banking sector, but they had not pursued it. Substantial concern remains that Anjouan, and possibly Moheli, allows shell banking activity.

There are reports that France, which as the former colonial power maintains substantial influence and activity in Comoros, has bypassed the Union and island governments in order to, where possible, prosecute suspects in money laundering or shell banks under French law. Although Comoros lacks homegrown narcotics, the islands are used as a transit site for drugs coming mainly from Madagascar.

In view of international concern about drug trafficking, in 1993 France began providing technical expertise in this field to Comoros.

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, license insurance companies, internet casinos, and international business companies (IBC's). Moheli claims to have licensed over 1200 IBC's. Bearer shares of IBC's are permitted under Moheli law. Anjouan also forms trusts, and registers aircraft and ships (without requiring an inspection of the aircraft or ship in Anjouan).

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 has become the 12th member of the free-trade area of the Common Market for Eastern and Southern Africa (Comesa). The U.S. Export-Import Bank (ExIm Bank) has added Comoros to its Short-Term Insurance Pilot Program for Africa (STIPP), while renewing the program for three years, beginning March 31, 2006.

The Government of the Union of the Comoros (GOC) should harmonize anti-money legislation for the three islands that comprise the federal entity. The legislation should adhere to world standards. A unified financial intelligence unit should be established and the unregulated offshore financial sectors in Moheli and Anjouan should either be regulated by federal authorities or be shut down. In either case, bearer shares should be prohibited. The list of individuals and entities that are included on the United Nations 1267 Sanctions Committee's consolidated list should be circulated to banks in the Comoros. The deficiencies in the anti-money laundering/terrorist financing regimes in the Comoros and the inability to implement existing legislation make it vulnerable to traditional money laundering and to the financing of terrorism. Comoros should make every effort to comport to international standards.

Cook Islands

The Cook Islands is a self-governing parliamentary democracy in free association with New Zealand and a member of the British Commonwealth. Cook Islanders are citizens of New Zealand. The Cook Islands' offshore sector makes it vulnerable to money laundering. The sector offers banking, insurance, international trusts, and formation of international business companies and trusts. However, due to recent legislative and regulatory changes, the Cook Islands complies 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, nonperforming loans made by the Cook Islands Development Bank have been transferred to another affiliated company. In addition to the three domestic banks, the Cook Islands financial sector also consists of four international banks, six trustee companies, and six offshore and three domestic insurance companies.

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 often contain a "flee clause." 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" is used to transfer APTs in times of emergency, such as a natural disaster.

The Cook Islands was placed on the Financial Action Task Force (FATF) list of Non-Cooperative Countries and Territories (NCCT) since 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. 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) 2003 and additional legislation and amendments in 2003 and 2004, Cook Islands authorities strengthened its anti-money laundering and counterterrorist financing (AML/CTF) legal and institutional framework. Reviews are underway to consider how the AML/CTF legislation affects other domestic laws. The Financial Supervisory Commission (FSC), regulator of the licensed financial sector, drafted new insurance legislation in 2006. It is anticipated that the draft legislation will be passed in 2007. The legislation will regulate 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 and money remitters. 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). The CIFIU is also responsible for assessing compliance by nonlicensed institutions.

The CIFIU is the central unit responsible for processing disclosures of financial information in accordance with anti-money laundering and antiterrorist financing legislation. It became fully operational with the assistance of a Government of New Zealand technical advisor. The FTRA 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.

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 Minister of Finance, who is responsible for administrative oversight, appoints the head of the CIFIU.

The CIFIU is participating in the Pacific FIU database project (PFIUDP) provided by AUSTRAC, the Australian FIU. The CIFIU received a prototype of the database and is now testing the reporting and analysis capacity. The Pacific FIU Database Project includes other jurisdictions that will receive versions of the same database framework.

Since June 2004 the Cook Islands had made further progress in implementing its AML/CFT 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/CFT issues; and enables government agencies to share information and training resources gathered from their regional and international networks. The AML/CFT 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/CFT 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 GOCI 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. The Cook Islands is an active member of the Asia/Pacific Group on Money Laundering (APG), an associate member organization of the FATF. The CIFIU became a member of the Egmont Group in June 2004, has bilateral agreements allowing the exchange of financial intelligence with Australia, and is negotiating a memorandum of understanding (MOU) with Thailand. 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 also 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 received nine requests for mutual legal assistance since the Mutual Assistance in Criminal Matters Act came into force in 2003. Five have been answered, and four 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 should continue to implement legislation designed to strengthen its nascent AML/CTF institutions. 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 comports with international standards.

Costa Rica

Costa Rica is not a major financial center but remains vulnerable to money laundering and other financial crimes. This is due in part to narcotics trafficking in the region, particularly of South American cocaine, and the presence in Costa Rica of Internet gaming companies. Costa Rica has a black market for smuggled goods, but the goal of most of this activity seems to be tax evasion rather than laundering of narcotics proceeds. Reforms in 2002 to the Costa Rican counternarcotics law expand the scope of anti-money laundering regulations, but also create an invitation to launder funds by eliminating the government's licensing and supervision of casinos, jewelers, realtors, attorneys, and other nonbank financial institutions. No actions were taken to close this loophole in 2006. Gambling is legal in Costa Rica, and there is no requirement that the currency used in Internet gaming operations be transferred to Costa Rica. Currently, over 250 sports-book companies have registered to operate in Costa Rica. Two of the largest companies shut down their operations during 2006 when top executives were arrested in the United States.

In 2002, the Government of Costa Rica (GOCR) enacted Law 8204. Law 8204 criminalizes the laundering of proceeds from all serious crimes, which are defined as crimes carrying a sentence of four years or more. Law 8204 also obligates financial institutions and other businesses (such as money exchangers) to identify their clients, report currency transactions over $10,000 and suspicious transactions to the financial intelligence unit (FIU), keep financial records for at least five years, and identify the beneficial owners of accounts and funds involved in transactions. While Law 8204, in theory, applies to the movement of all capital, current regulations are strictly interpreted so that the law applies only to those entities that are involved in the transfer of funds as a primary business purpose. Therefore, the law does not cover such entities as casinos, dealers in gems or Internet gambling operations, as their primary business is not the transfer of funds.

The formal banking industry in Costa Rica is tightly regulated. However, the offshore banking sector, which offers banking, corporate and trust 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. Costa Rican authorities acknowledge that they are unable to adequately assess risk. Costa Rican financial institutions are regulated by the Office of the Superintendent of Financial Institutions (SUGEF).

Currently, six offshore banks maintain correspondent operations in Costa Rica: three from The Bahamas and three from Panama. The GOCR has supervision agreements with its counterparts in Panama and The Bahamas, permitting the review of correspondent banking operations. These counterpart regulatory authorities occasionally interpret the agreements in ways that limit review by Costa Rican officials. In 2005, the GOCR's Attorney General ruled that the SUGEF lacks authority to regulate offshore operations due to an apparent contradiction between the 1995 Organic Law of the

Costa Rican Central Bank and Law 8204. Draft legislation to correct the contradiction and reassert the SUGEF's regulatory power is under review in the Legislative Assembly. However, the Legislative Assembly took no action on this draft legislation in 2006.

All persons carrying cash are required to declare any amount over $10,000 to Costa Rican officials at ports of entry. During 2006, officials seized over $5.2 million in narcotics-related assets, much of it in undeclared cash. By comparison, in 2005 the GOCR seized $850,000 in assets. Seized assets are processed by the Costa Rican Drug Institute (ICD) and if forfeited, are divided among drug treatment agencies (60 percent), law enforcement agencies (30 percent), and the ICD (10 percent).

Eighteen free trade zones operate within Costa Rica, primarily producing electronics, integrated circuits, textiles and medicines for re-export. The zones are under the supervision of "PROCOMER" a federal export-promotion entity. Costa Rican authorities report no indications of trade-based money laundering schemes in the zones. PROCOMER strictly enforces control over the zones, but its measures are aimed primarily at preventing tax evasion.

Costa Rica's FIU, the Unidad de Análisis Financiero (UAF), became operational in 1998 and was admitted into the Egmont Group in 1999. Established within the ICD, the UAF analyzes suspicious activity reports for potential referral to prosecutors. It has no regulatory responsibilities. The UAF has access to the records and databases of financial institutions and other government entities, but must obtain a court order if the information collected is to be used as evidence in court. The banking industry cooperates with authorities and routinely reports suspicious activities. In spite of its broad access to government information and high levels of cooperation with the financial sector, the UAF remains ill-equipped and under-funded to provide information needed by investigators. Nevertheless, in 2006, the UAF increased the quality of its analysis and forwarded more thoroughly analyzed cases to prosecutors. Three money laundering cases that began judicial proceedings in 2005 were successfully prosecuted in 2006.

Although the GOCR has ratified the major UN counterterrorism conventions, terrorism and its financing are not crimes in Costa Rica. Costa Rican authorities have received and circulated 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 E.O. 13224. However, these authorities cannot block, seize, or freeze property without prior judicial approval. Thus, 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 2006.

In 2002, a government task force drafted a comprehensive counterterrorism law with specific terrorist financing provisions. The draft law, when passed, would expand existing conspiracy laws to include the financing of terrorism and enhance existing narcotics laws by incorporating the prevention of terrorist financing into the mandate of the ICD. In 2004, the Legislative Assembly also considered a separate draft terrorism law but took no action. In 2006, the Assembly's Narcotics Committee continued to study the two proposals, but no further progress has been made.

Costa Rica is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. The GOCR has signed, but not yet ratified, the UN Convention against Corruption. The GOCR has also signed the Organization of American States (OAS) Inter-American Convention on Mutual Assistance in Criminal Matters, and has ratified the Inter-American Convention against Terrorism. Costa Rica is a member of the Caribbean Financial Action Task Force (CFATF) and the Money Laundering Experts Working Group of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD). The UAF is a member of the Egmont Group.

Even though Costa Rica has convicted a handful of individuals for money laundering in 2005 and 2006, further efforts are required to bring Costa Rica into compliance with international anti-money laundering and counterterrorist financing standards. The GOCR should pass legislation that clarifies contradictions regarding the supervision of its offshore banking sector, and should extend its anti-money laundering legislation and regulations to cover the Internet gaming sector, gem dealers, attorneys, casinos and other nonbank financial institutions. Costa Rica should also criminalize terrorism and terrorist financing, and ensure that its financial intelligence unit and other GOCR authorities are adequately equipped to combat financial crime.

Côte d'Ivoire

Cote d'Ivoire is an important West African regional financial hub. Money laundering and terrorist financing in Cote d'Ivoire are 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. 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, respect for the rule of law continues to deteriorate. As a result, Ivorian and some Liberian nationals are becoming more and more involved in criminal activities and the subsequent laundering of funds. Cote d'Ivoire is ranked 153 out of 163 countries in Transparency International's 2006 Corruption Perception Index.

The outbreak of the rebellion in 2002 increased the amount of smuggling of goods across the northern borders, especially of textiles and cigarette products. There have also been reports of an increase in the processing and smuggling of small quantities of diamonds from mines located in the north. Ivorian law enforcement authorities have no control over the northern half of the country, and therefore they cannot judge what relationship, if any, the funding for smuggled goods might have to narcotics proceeds or other illicit proceeds. Smuggling of sugar, cotton, cocoa, cars, and pirated DVDs occurs in the government-controlled south and is motivated by a desire to avoid the payment of 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 contraband funds that are laundered into the banking system via informal moneychangers. Criminal enterprises use both the formal and informal financial sector to launder funds. Cash is moved both via the formal banking sector and by cash couriers. Cash earned by immigrant or migrant workers generally flows out of Cote d'Ivoire, going to extended families outside the region. Informal money couriers and money transfer organizations similar to hawaladars move funds both domestically and within the sub-region. Currently, domestic informal cash transfer systems are not regulated. Informal remittance transfers from outside Cote d'Ivoire violate West African Central Bank (BCEAO) money transfer regulations. Because of the division of the country, a lack of security, and the lack of a widespread banking system, transportation companies have also stepped in to provide courier services. The standard fee for these services is approximately ten percent. In addition to transferring funds, criminal enterprises launder illicit funds by investing in real estate and consumer goods such as used cars in an effort to conceal the source of funding.

Hizbollah is present in Cote d'Ivoire, and it 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. In August 2004, the Ivorian government adopted a plan for the creation of a free trade zone for information technology and for biotechnology. This project is dormant. Another free trade zone project, which was planned for the port of San Pedro, also remains dormant.

The Economic and Financial police have noticed an increase in financial crimes related to credit card theft and foreign bank account fraud, which includes wire transfers of large sums of money primarily involving British and American account holders who are the victims of Internet based advanced fee scams. The Ministry of Finance remains concerned by the high levels of tax fraud, particularly VAT tax fraud, by merchants. The country has the largest bank network in the region with seventeen banks and two nonbank financial institutions. Of that number, there are eight foreign-owned banks and two foreign-owned financial institutions in operation. French banking accounts for more than 60 percent of banking activity. The law requires a capitalization of the CFA equivalent of $2 million for banks and $600,000 for financial institutions. Banks provide traditional banking services such as lending, savings and checking accounts and money transfers, while financial institutions offer leasing, payroll and billing services, and project financing for small businesses. The political crisis has disrupted banking operations.

The Ivorian banking law, enacted in 1990, prevents disclosure of client and ownership information, but it 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.

Until recently, the penal code criminalized only money laundering related to drug-trafficking, fraud, and arms trafficking. On November 29, 2005, the Ivorian National Assembly adopted the West African Economic and Monetary Union's (WAEMU) model law on money laundering, making money laundering per se a criminal offense. Money laundering is defined as the intention to conceal the criminal origins of illicit funds. The new law was adopted on December 2, 2005, and became effective on August 9, 2006.

The new law focuses on the prevention of money laundering and also expands the definition of money laundering to include the laundering of funds from all serious crimes. The law does not set a minimum threshold. It includes standard "know your customer" requirements for banks and other financial institutions. It establishes procedures, which require these institutions to assist in the detection of money laundering through suspicious transaction reporting, and it creates an Ivorian Financial Intelligence Unit (FIU). It also provides a legal basis for international cooperation. The new law includes both penal and civil penalties. The law permits the freezing and seizure of assets, which includes instruments and proceeds of crime, including business assets and bank accounts that are used as conduits for money laundering. Substitute assets cannot be seized if there is no relationship with the offense. Legitimate businesses can be seized if used to launder money or support terrorist or other illegal activities.

Under the new money laundering law, Cote d'Ivoire is required to create and fund an FIU named the "Cellule Nationale de Traitement des Informations Financieres" (CENTIF). The CENTIF will report to the Finance Ministry. On a reciprocal basis, with the permission of the Ministry of Finance, the CENTIF may share information with the FIUs in member states of WAEMU or with those of non-WAEMU countries, as long as those institutions keep the information confidential.

The FIU will take the lead in tracking money laundering, but it will continue to work 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 will still continue their missions, which include fiscal and customs fraud and counterfeiting. The Ivorian Economic and Financial police, the criminal police unit (Police Judiciaire), the Department of Territorial Surveillance (Ivorian intelligence service), the CRF and ANSI all are responsible for investigating financial crimes, including money laundering and terrorist financing. However, in addition to a lack of resources for training, there is a perceived lack of political will to permit investigative independence.

The Ministry of Finance, the BCEO, and the West African Banking Commission, headquartered in Cote d'Ivoire, supervise and examine Ivorian compliance with anti-money laundering/counterterrorist financing laws and regulations. All Ivorian financial institutions are now required to begin to maintain customer identification and transaction records for ten years. For example, all bank deposits over approximately CFA 5,000,000 (approximately $10,000) made in BCEAO member countries must be reported to the BCEAO, along with customer identification information. Law enforcement authorities can access these records to investigate financial crimes upon the request of a public prosecutor. In 2005, there were no arrests or prosecutions for money laundering or terrorist financing.

The new legislation imposes a ten year retention requirement on 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 occasional customers, the floor value for "significant transactions" is CFA 5,000,000.

The new money laundering controls will 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, businesses, and professionals and nonbank institutions under the scope of the new 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 WAEMU administrative regulation R/09/98/CM/WAEMU. There is no separate domestic law or regulation. When traveling from Cote d'Ivoire to another WAEMU country, Ivorian and expatriate residents must declare the amount of currency being carried out of the country. When traveling from Cote d'Ivoire to a destination other than another 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.

Although Cote d'Ivoire's new money laundering law encompasses the laundering of funds from all serious crimes, terrorism and terrorist financing are not considered "serious crimes" for the purposes of this law. Cote d'Ivoire does not have a specific law that criminalizes terrorist financing, as required under UNSC resolution 1373. Until the passage of the new law, the GOCI relied on several WAEMU directives on terrorist financing, which provided a legal basis for administrative action by the Ivorian government to implement the asset freeze provisions of UNSCR 1373. The BCEAO and Ivorian 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. A U.S. financial institution present in Cote d'Ivoire confirms the receipt of notices issued by government authorities. No assets related to terrorist entities or individuals have been discovered, frozen or seized.

Cote d'Ivoire participates in the ECOWAS-Intergovernmental Group for Action Against Money Laundering (GIABA) based in Dakar, which sits as an observer to the Financial Action Task Force (FATF). In July 2006, the United Nations Office on Drugs and Crime (UNODC) sponsored a meeting on money laundering in cooperation with the GIABA. The Ivorian government has neither adopted laws nor promulgated regulations that specifically allow for the exchange of records with United

States on money laundering and terrorist financing. However, under the new money laundering law, after obtaining the approval of the Finance Ministry, the CENTIF could share information related to money laundering records with U.S. or other countries on a reciprocal basis and under an agreement of confidentiality between the two governments.

Cote d'Ivoire has demonstrated a willingness to cooperate with the USG in investigating financial or other crimes. For example, in one case from 2004, an American citizen was being defrauded by an individual posing as a GOCI Customs Official requesting demurrage fees for a shipment of goods. With a short window of opportunity for action, the U.S. Embassy notified the Economic Police, who then instructed the Bank Examiner to monitor the suspect's account. The next morning, the Economic Police arrested a Nigerian who came in to retrieve the funds. Armed with a search warrant, the police searched the suspect's house, gathered evidence of a boiler-room operation, and arrested three other Nigerians. The funds ($15,000) were successfully wired back to the victim.

Cote d'Ivoire hosted a workshop and conference regarding money laundering and fraud prevention, both in March 2006. Abidjan also hosted the Eleventh Conference of Customs Director Generals for West and Central Africa on information exchange as a critical part of the fight against customs and fiscal fraud. Also in March 2006, Cote d'Ivoire held, in collaboration with the United Nations Development Program (UNDP), a workshop releasing the results of the 2004 training seminar on financial delinquency, money laundering and terrorism financing.

Cote d'Ivoire is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the 1988 UN Drug Convention. Cote d'Ivoire has signed, but not yet ratified, the UN Convention against Transnational Organized Crime.

The Government of the Cote d'Ivoire should implement its new anti-money laundering law, including the funding and establishing of an FIU. It should criminalize terrorist financing. Cote d'Ivoire law enforcement and customs should examine forms of trade-based money laundering and informal value transfer systems. Authorities should take steps to halt the spread of corruption that permeates both commerce and government and facilitates the underground economy and money laundering. Cote d'Ivoire should ratify the UN Convention against Transnational Organized Crime.

Cyprus

Cyprus has been divided since the Turkish military intervention of 1974, following a coup d'etat directed from Greece. Since then, the southern part of the country (approximately sixty percent of the country) has been under the control of the Government of the Republic of Cyprus. The northern forty percent is controlled by a Turkish Cypriot administration that in 1983 proclaimed itself the "Turkish Republic of Northern Cyprus (TRNC)," recognized only by Turkey. The U.S. Government recognizes only the Government of the Republic of Cyprus (GORC).

The government-controlled area of the Republic of Cyprus is a major regional financial center with a robust financial services industry that includes an offshore sector. As with other such centers, Cyprus remains vulnerable to international money laundering activities. Fraud and other financial crimes, and narcotics trafficking are the major sources of illicit proceeds laundered in Cyprus. Casinos and internet gaming sites are not permitted, although sports betting halls are allowed.

A number of factors facilitated the development of Cyprus' offshore financial sector in Cyprus: 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 particularly well trained in legal and accounting skills; a sophisticated telecommunications infrastructure; and, relatively liberal immigration and visa requirements. Since the offshore financial sector was established in 1975, more than 54,000 offshore international business companies have been registered. Reportedly, there are approximately 14,000 international business companies (IBCs) are

currently registered. An International Banking Unit (IBU) is a Cypriot limited liability company or a branch of a foreign bank, which has obtained a banking license from the Central Bank. An Offshore Financial Services Company (OFSC) engages in dealing, buying, selling, subscribing to or underwriting investments; managing investments belonging to other persons; giving investment advice to actual or potential investors; and establishing collective investment schemes. The Central Bank vetting process for offshore companies also ensures that prospective OFSCs are linked to existing investment or financial services companies in well-regulated countries.

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 are now taxed at a uniform rate of 10 percent, irrespective of the permanent residence of their owners or whether they do business internationally or in Cyprus. A transition period allowing preferential tax treatment to offshore companies that existed prior to 2002 expired on January 1, 2006. Additionally, the prohibition from doing business domestically has been lifted and companies formerly classified as offshore are now free to engage in business locally. Bearer shares have been abolished .It is not clear whether the beneficial owners of the more than 50,000 international business companies formally registered in the offshore sector are now known to the Cyprus authorities.

The GORC continues to revise its anti-money laundering (AML) framework to meet evolving international standards. In 1996, the GOC passed the Prevention and Suppression of Money Laundering Activities Law, which mandated the establishment of the Cypriot financial intelligence unit (FIU). This law criminalizes all money laundering, provides for the confiscation of proceeds from serious crimes, and codifies the actions that banks, nonbank financial institutions, and obligated nonfinancial businesses must take, including those related to customer identification. The anti-money laundering law authorizes criminal (but not civil) seizure and forfeiture of assets. Subsequent amendments to the 1996 law broadened its scope by replacing the separate list of predicate offenses with a definition of predicate offense to be any criminal offense punishable by a prison term exceeding one year, by addressing government corruption, by providing for the sharing of assets with other governments and by facilitating the exchange of financial information with other FIUs.

Amendments passed in 2003 and 2004 authorize the FIU to instruct banks to delay or prevent execution of customers' payment orders; extend due diligence and reporting requirements to auditors, tax advisors, accountants, and, in certain cases, attorneys, real estate agents, and dealers in precious stones and gems; and permit administrative fines of up to 2863 Cypriot pounds (approximately$6,390). The amendments also increase bank due diligence obligations concerning suspicious transactions and customer identification requirements, subject to supervisory exceptions for specified financial institutions in countries with equivalent requirements.

Also in 2003, the GORC enacted legislation regulating capital and bullion movements and foreign currency transactions. The law requires all persons entering or leaving Cyprus to declare all currency, Cypriot or foreign, or gold bullion worth approximately $15,500 (approximately 6730 Cypriot pounds) or more. This sum is subject to revision by the Central Bank. This law replaced the exchange control restrictions under the Exchange Control Law, which expired in May 2004.

Four authorities regulate and supervise financial institutions in Cyprus: the Central Bank of Cyprus, responsible for supervising locally incorporated banks as well as subsidiaries and branches of foreign banks; the Cooperative Societies Supervision and Development Authority (CSSDA), supervising cooperative credit institutions; the Superintendent for Insurance Control; and the Cyprus Securities and Exchange Commission. Designated nonfinancial businesses and professions (DNFBPs) are regulated by three entities: the Council of the Bar Association supervises attorneys; the Institute of Certified Public Accountants supervises accountants; and the 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's anti-money laundering laws and regulations.

The GORC-controlled area of Cyprus currently hosts a total of 40 banks. Fourteen of these are incorporated locally. Eleven of the fourteen banks are commercial banks and three are specialized financial institutions. Of the commercial banks, six are foreign-owned, and two are branches of foreign banks. The remaining 26 banks are foreign-incorporated and conduct their operations almost exclusively outside of Cyprus. At the end of August 2006, the cumulative assets of domestic banks were $53.9 billion, while the cumulative assets of subsidiaries and branches of the foreign-incorporated banks were $22.8 billion.

As of May 2004, when Cyprus joined the EU, banks licensed by competent authorities in EU countries could establish branches in Cyprus or provide banking services on a cross-border basis without obtaining a license from the Central Bank of Cyprus, under the EU's "single passport" principle. By the end of 2006, four foreign banks were operating a branch in Cyprus under the EU's "single passport" arrangement.

Cyprus hosts six licensed money transfer companies, 40 international independent financial advisers, six international trustee services and 200 feeder funds. There are also 47 investment firms, two management firms handling "undertakings for collective investment in transferable securities" (UCITS), 43 licensed insurance companies, 238 licensed real estate agents, 1,858 registered accountants, 1,631 practicing lawyers and around 350 credit institutions. These 350-plus credit societies and cooperative savings banks retain 32 percent of total deposits.

In October 2006, the IMF released a detailed assessment of the "Observance of Standards and Codes for Banking Supervision, Insurance Supervision and Securities Regulation." Among other issues, the report noted that the SEC was legally unable to cooperate with foreign regulators if the SEC did not have an independent interest in the matter being investigated and that the SEC was experiencing difficulty obtaining information regarding the beneficial owners of Cypriot-registered companies. The SEC is working to resolve both of these issues. The report also noted that commitments emerging from EU accession had "placed stress on the skills and resources" of the staff of the CSSDA and the Insurance Superintendent and recommended additional training.

In recent years the Central Bank has introduced many new regulations aimed at strengthening anti-money laundering vigilance in the banking sector. Among other requirements, banks must (1) ascertain the identities of the natural persons who are the "principal/ultimate" beneficial owners of corporate or trust accounts; (2) obtain as quickly as possible identification data on the natural persons who are the "principal/ultimate" beneficial owners when certain events occur, including: an unusual or significant transaction or change in account activity; a material change in the business name, officers, directors and trustees, or business activities of commercial account holders; or a material change in the customer relationship, such as establishment of new accounts or services or a change in the authorized signatories; (3) adhere to the October 2001 paper of the Basel Committee on Banking Supervision on "Customer Due Diligence for Banks"; and (4) pay special attention to business relationships and transactions involving persons from jurisdictions identified by the Financial Action Task Force (FATF) as noncooperative. This list is updated regularly in line with the changes effected to the list of noncooperative countries and territories by the FATF.

All banks must report to the Central Bank, on a monthly basis, individual cash deposits exceeding 10,000 Cypriot pounds (approximately $22,000 in local currency) or approximately $10,000 in foreign currency. Bank employees are required to 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, and these are audited by the Central Bank as part of its regular on-site examinations. Banks must file monthly reports with the Central Bank indicating the total number of suspicious transaction reports (STRs) submitted to the compliance officer and the number

forwarded by the compliance officer to the FIU. By law, 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 transaction records for five years.

In November 2004, the Central Bank issued a revised money laundering guidance note that places several significant new obligations on banks, including requirements to develop a customer acceptance policy; renew customers' identification data on a regular basis; construct customers' business profiles; install computerized risk management systems in order to verify whether a customer constitutes a "politically exposed person"; provide full details on any customer sending an electronic transfer in excess of $1,000; and implement (by June 5, 2005) adequate management information systems for on-line monitoring of customers' accounts and transactions. Cypriot banks have responded by adopting dedicated electronic risk management systems, which they typically use to target transactions to and from high-risk countries. Cyprus's Exchange Control Law expired on May 1, 2004, ending Central Bank review of foreign investment applications for non-EU residents. Individuals wishing to invest on the island now apply through the Ministry of Finance. The Ministry also supervises collective investment schemes.

The Central Bank also requires compliance officers to file an annual report outlining measures taken to prevent money laundering and to comply with its guidance notes and relevant laws. In addition, the Central Bank is legally empowered to conduct unannounced inspections of bank compliance records. In July 2002, the U.S. Internal Revenue Service (IRS) officially approved Cyprus's "know-your-customer" rules, which form the basic part of Cyprus's anti-money laundering system. As a result of the above approval, banks in Cyprus that may be acquiring United States securities on behalf of their customers are eligible to enter into a "withholding agreement" with the IRS and become qualified intermediaries.

Established as the Cypriot FIU in 1997, the Unit for Combating Money Laundering (MOKAS) is responsible for receiving and analyzing STRs and for conducting money laundering or financial fraud investigations. At the time of the MONEYVAL mutual evaluation report submission, in February 2006, MOKAS had a multidisciplinary staff of 14. In June 2006, MOKAS hired an additional six financial investigators. A representative of the Attorney General's Office heads the unit. MOKAS cooperates closely with FinCEN and other U.S. Government agencies in money laundering investigations. 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 an increase in the number of STRs being filed from 25 in 2000 to 179 in 2006. During 2006, MOKAS received 208 information requests from foreign FIUs, other foreign authorities, and INTERPOL. MOKAS evaluates evidence generated by its member organizations and other sources to determine if an investigation is necessary. Money laundering is an autonomous crime. The MONEYVAL team noted at its on-site visit that there appeared to be 14 money laundering cases in the courts. Only three of the 14 known cases resulted from the STR process.

MOKAS has the power to suspend financial transactions for an unspecified period of time as an administrative measure. MOKAS also has the power to apply for freezing or restraint orders affecting any kind of property at a very preliminary stage of an investigation. In 2005, for the first time, MOKAS issued several warning notices, based on its own analysis, identifying possible trends in criminal financial activity. These notices have already produced results, including the closure of dormant bank accounts. MOKAS conducts anti-money laundering training for Cypriot police officers, bankers, accountants, and other financial professionals. Training for bankers is conducted in conjunction with the Central Bank of Cyprus.

During 2006, MOKAS opened 410 cases and closed 160. There were twelve prosecutions for money laundering, which resulted in seven convictions. During the same period, it issued 28 Information Disclosure Orders (typically involving judiciary proceedings in courts abroad), 13 administrative orders for postponement of transactions, and 4 freezing orders, including two foreign restraint orders, resulting in the freezing of 2.23 million euros (approximately $2.9 million) in bank accounts and three vehicles. . Additionally, during 2006, MOKAS issued one confiscation order for a total amount of 1.33 million euros (approximately $1.73 million). A number of other cases are pending.

On November 30, 2001, Cyprus became a party to the UN International Convention for the Suppression of the Financing of Terrorism. Terrorism financing is criminalized by sections 4 and 8 of the Ratification Law 29 (III) of 2001. The implementing legislation amended the AML law to criminalize the collection of funds in the knowledge that these 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 terrorism finance offenses. However, as noted in the 2006 MONEYVAL mutual evaluation report, Cyprus has yet to criminalize the general collection of funds in the knowledge that they would be used by terrorists or terrorist groups for any purpose (i.e. not just for violent acts) as required by FATF Special Recommendation II. In November 2004, MOKAS designated two employees to be responsible for terrorist finance issues. 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 a 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 by the UN 1267 Sanctions Committee or the EU Clearinghouse as a terrorist of terrorist organization. If a financial institution were to find any matching accounts, it would be required to immediately freeze the accounts and inform the Central Bank. As of January 2007, no bank had reported holding a matching account. When FIUs or governments such as the USG—not the UN or the EU Clearinghouse—designate and circulate the names of suspected terrorists, MOKAS has the authority to block funds and contacts commercial banks directly to investigate. None of these checks have revealed anything suspicious to date. The lawyers' and accountants' associations cooperate closely with the Central Bank. The GORC cooperates with the United States to investigate terrorist financing. MOKAS reports that no terrorist assets have been found in Cyprus to date and thus there have been no terrorist finance prosecutions or freezing of terrorist assets. However, authorities reported that in 2006 there had been one investigation for terrorism financing involving four persons.

Reportedly, there is no evidence that alternative remittance systems such as hawala or black market exchanges are operating in Cyprus on a significant scale. The GORC believes that its existing legal structure is adequate to address money laundering through such alternative systems. The GORC licenses charitable organizations, which must file with the GORC copies of their organizing documents and annual statements of account. Reportedly, the majority of charities registered in Cyprus are domestic organizations.

Cyprus is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. Cyprus is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) and the Offshore Group of Banking Supervisors. 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.

Cyprus underwent a MONEYVAL mutual evaluation in April 2005, the results of which were published in a report adopted at the MONEYVAL Plenary meeting in February 2006. The report

found Cyprus to be fully compliant in 17 areas, largely compliant in 22, and partially compliant in 10 of the Financial Action Task Force's (FATF) Forty Recommendations and Nine Special Recommendations on terrorism finance. There were no criteria for which Cyprus was found to be noncompliant. The assessment team also put forward a detailed recommended action plan designed to further improve its anti-money laundering system.

The Government of the Republic of Cyprus (GORC) has put in place a comprehensive anti-money laundering regime. It should continue to take steps to tighten implementation of its laws. In particular, it should enhance regulation of corporate service providers, including trust and incorporation companies, lawyers, accountants, and other designated nonfinancial businesses and professions. Now that the GOC is abolishing its offshore financial services, it should withdraw from the Offshore Group of Banking Supervisors to dispel any confusion that its continued membership might engender. It should enact provisions that allow for civil forfeiture of assets. It should also continue to work on improving the collection and centralization of statistical data in relation to money laundering investigations, prosecutions and convictions. Cyprus should criminalize the collection of funds with the knowledge that they will be used by terrorists or terrorist groups for any purpose—not only to commit violent acts. Cyprus should also take steps to implement the recommendations of the recent MONEYVAL and IMF evaluations, including ensuring the staffing level at MOKAS is sufficient for MOKAS to fulfill its mandate.

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. It is thought that the 19 essentially unregulated and primarily Turkish-mainland owned casinos and the 15 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 change 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. Another area of concern is the approximately five hundred "finance institutions" operating in the area that extend credit and give loans. Although they must register with the "Office of the Registrar of Companies," they are unregulated. Some of these companies are owned by banks and others by auto dealers. In 2005 and 2006, there was a large increase in the number of sport betting halls, which are licensed by the "Office of the Prime Minister." There are currently seven companies operating in this sector, with a total of 85 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 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 staff. Nevertheless, several other casinos are still believed to have significant links to organized crime groups in Turkey.

The fact that the TRNC is recognized only by Turkey limits the ability of Turkish Cypriot officials to receive training or funding from international organizations with experience in combating money laundering. The Turkish Cypriot community is not part of any regional FATF-style organization and thus is not subject to any peer evaluations.

The offshore banking sector remains a concern. In August 2004, the U.S. Department of the Treasury's FinCEN issued a notice of proposed rulemaking to impose a special measure against First Merchant Bank OSH Ltd in the area administered by Turkish Cypriots as a financial institution of primary money laundering concern. Pursuant to Section 311 of the USA PATRIOT Act, FinCEN found First Merchant Bank to be of primary money laundering concern based on a number of factors, including: (1) it is licensed as an offshore bank in the TRNC, a jurisdiction with inadequate anti-money laundering controls, particularly those applicable to its offshore sector; (2) it is involved in the marketing and sale of fraudulent financial products and services; (3) it has been used as a conduit for the laundering of fraudulently obtained funds; and (4) the individuals who own, control, and operate

First Merchant Bank have links with organized crime and apparently have used First Merchant Bank to launder criminal proceeds. As a result of the finding and in consultation with federal regulators and the Departments of Justice and State, FinCEN proposed imposition of the special measure that would prohibit the opening or maintaining of correspondent or payable-through accounts by any U.S. domestic financial institution or domestic financial agency for, or on behalf of, First Merchant Bank OSH Ltd. On December 4, 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 limited steps to address these risks. Nevertheless, it appears that the Turkish Cypriot leadership lacks the political will necessary to push through reforms needed to introduce effective oversight of its limited and relatively isolated financial sector. In 1999, an anti- money laundering law (AMLL) for the area administered by Turkish Cypriots went into effect with the stated aim of reducing the number of cash transactions in the TRNC as well as improving the tracking of any transactions above $10,000. Banks are required to report to the "Central Bank" 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. Banks, nonbank financial institutions, and foreign exchange dealers must report all currency transactions over $20,000 and suspicious transactions in any amount. Banks must follow a know-your-customer policy and require customer identification. Banks must also submit suspicious transaction reports (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. However, the AMLL has never been fully implemented or enforced.

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 reportedly 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 officials lack the technical skills needed to investigate and prosecute financial crimes.

Although the 1999 AMLL prohibits individuals entering or leaving the area administered by Turkish Cypriots from transporting more than $10,000 in currency without prior Central Bank authorization, Central Bank officials note that this law is difficult to enforce, given the large volume of travelers to and from Turkey. In 2003, 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 Ministries of Finance, Economy and Tourism are drafting several new anti-money laundering laws that they claim will, among other things, establish an FIU and provide for better regulation of casinos, currency exchange houses, and both onshore and offshore banks. Turkish Cypriot officials have committed to ensuring that the new legislation meets international standards. However, it is unclear if or when the new legislation will be adopted, and if it is adopted, whether it will ever be fully implemented and enforced. Work on the new bills has been ongoing for more than two years.

There are currently 23 domestic banks in the area administered by Turkish Cypriots. Internet banking is available. The offshore sector consists of 16 banks and approximately 50 companies. The offshore banks may not conduct business with residents of the area administered by Turkish Cypriots and may

not deal in cash. The offshore entities are audited by the Central Bank and are required to submit a yearly report on their activities. However, the Central Bank has no regulatory authority over the offshore banks and can neither grant nor revoke licenses. Instead, the Ministry of Finance performs this function. Since 2000, the Turkish Cypriot authorities have registered one new offshore bank. A new law has come into effect that restricts the granting of new bank licenses to only those banks with licensees in an OECD country or a country with "friendly relations" with the TRNC.

The 1999 Turkish Cypriot AMLL provided better banking regulations than were previously in force, 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 that 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 enact a new anti-money laundering law, establish a strong, functioning financial intelligence unit, and adopt and implement a strong regulatory environment for all obliged institutions, in particular casinos, money exchange houses, and entities in the offshore sector. 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, the more efficient STR reporting, better analysis of reports, and enhanced use of legal tools available for prosecutions.

Czech Republic

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 source of laundered assets in the country, Czech officials and media outlets have voiced increasing 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, currency exchanges, 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 major problem.

The Czech Republic first criminalized 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 introduce a new independent offense called "Legalization of Proceeds from Crime." This offense has a wider scope than previous provisions in that it enables prosecution for laundering one's own illegal proceeds (as opposed to those of other parties). The 2002 amendment also stipulated punishments of five to eight years imprisonment for the legalization of proceeds from all serious criminal activity and also called for the forfeiture of assets associated with money laundering.

The Czech anti-money laundering legislation (Act No. 61/1996, Measures Against Legalization of Proceeds from Criminal Activity) became effective in July 1996. A 2000 amendment to the money laundering law requires a wide range of financial institutions to report all suspicious transactions to the Czech Republic's financial intelligence unit (FIU), known as the Financial Analytical Unit (FAU) of the Ministry of Finance. In September 2004, the latest amendments to the money laundering law came into force. The amendments introduced several major changes to the Czech Republic's money laundering laws and harmonized the nation's legislation with the requirements of the Council Directive 2001/97/EC on prevention of the use of the financial system for money laundering (European Union's Second Money Laundering Directive). As a result, the list of covered institutions

now includes attorneys, casinos, realtors, notaries, accountants, tax auditors, and entrepreneurs engaging in transactions exceeding 15,000 euros (approximately $19,440).

The Ministry of Interior is currently drafting legislation implementing the European Union's Third Money Laundering Directive. In connection with this effort, the Czech National Bank is preparing an amendment to the foreign currency law that would introduce new regulations and licensing requirements for currency exchanges. Moreover, new legislation on the "Application of International Sanctions" came into force in April 2006. Under the new law, the FAU has the authority to fine institutions not reporting 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 with the new law.

The Czech Republic had been criticized in the past for allowing anonymous passbook accounts to exist within the banking system. Legislation adopted in 2000 prohibits new anonymous passbook accounts. In 2002, the Act on Banks was amended to abolish all existing bearer passbooks by December 31, 2002, and by June 2003 approximately 400 million euros had been converted to nonbearer passbooks. While account holders can still withdraw money from the accounts for the next decade, the accounts do not earn interest and cannot accept deposits. In 2003, the Czech National Bank introduced new "know your customer" measures, based on the recommendations of both the Financial Action Task Force (FATF) and the Basel Committee, and created an on-site inspection team. New due diligence provisions became effective in January 2003.

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 anti-money laundering act, anyone seeking to enter or leave the Czech Republic with more than 15,000 Euros in cash, traveler's checks, or other monetary instruments must declare this to customs officials, who are required to forward this information to the FAU. Similar reporting requirements apply to anyone seeking to mail the same amount in cash into or out of the country. In practice, however, the effectiveness of these procedures is difficult to assess. With the accession of the Czech Republic to the EU in 2004, nearly all customs stations on the borders were closed. Although the customs station at the Prague Airport remains operational, detecting the smuggling or transport of large sums of currency by highway is difficult. Reportedly, Chinese and Vietnamese residing locally in the Czech Republic are the most active in cash smuggling across the border.

Since 2000, financial institutions have been required to report all suspicious transactions to the FAU. As the Czech FIU, the FAU has the statutory authority to enforce money laundering and terrorist finance laws. The 2004 amendments to the Anti-Money Laundering Act extended the anti-money laundering/counterterrorist financing responsibilities of the FAU. As a result, the FAU is now authorized to share all information with the Czech Intelligence Service (BIS) and Czech National Security Bureau (NBU) in addition to its ongoing cooperation with the police and customs. It is hoped that this type of information sharing will improve the timeliness and nature of exchanges between the different agencies within the Czech government.

The FAU is an administrative FIU without law enforcement authority and can only investigate accounts for which designated entities have filed suspicious transaction reports. The FAU has the power to ask the banking sector to check a specific individual or organization's account. Since April 2006, they are also able to fine financial institutions for not reporting on accounts or other assets belonging to individuals, organizations, or countries on which international sanctions have been imposed. The FAU has neither the mandate nor the capacity to initiate or conduct criminal investigations. Investigative responsibilities lie with the Financial Police or other Czech National Police body.

There are two law enforcement agencies working closely together on the investigation of money laundering cases. The Financial Police (also known as the Illegal Proceeds and Tax Crime Unit) is the main law enforcement counterpart to the FAU and is also responsible for investigating cases of terrorism financing. The Unit for Combating Corruption and Financial Criminality (UOKFK) has primary responsibility for all financial crime and corruption cases.

Although the FAU conducts investigations based on suspicious transaction reports filed by financial institutions, these examinations only cover a relatively small segment of total financial activity within the Czech Republic. Moreover, the FAU's primary responsibility has been, and remains, identifying cases of tax evasion, which is an endemic problem in the Czech Republic. Recently, the FAU has focused on the growing problem of embezzlement of European Structural Funds and has already seized 220 million crowns (approximately $10 million) of suspected embezzled funds. The law facilitates 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 72 hours in order to give the FAU sufficient time to investigate whether or not 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 the Financial Police, which have another three days to gather the necessary evidence. If the Financial Police are 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 Financial Police fail 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 individuals or organizations on the UN 1267 Sanctions Committee's consolidated list of suspected terrorists and terrorist organizations. The FAU also has the ability to freeze assets associated with suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list.

While the institutional capacity to detect, investigate, and prosecute money laundering and financial offenses has unquestionably increased in recent years, both the FAU and the Financial Police face staffing challenges. Despite recommendations from both the FATF and the Council of Europe's FATF-style regional body (MONEYVAL) regarding the need for FAU staff increases, the government lowered its funding and personnel authorizations in 2005. The FAU still remains a relatively small organization, given the scope of its responsibilities. The Financial Police could soon face similar challenges due to changes in the police retirement plan and a perceived lack of political support for independent police work. Reportedly, many senior officers are leaving the police force or to considering early retirement. The departure of senior officials would have devastating effects and would hinder not only the Financial Police, but the organized crime unit, anticorruption unit, and other critical police organizations as well. Most troubling is the proposed dissolution of the Financial Police into other police units. The creation of the Financial Police was based on EU recommendations and these changes would possibly lead to a loss of EU funding and would negatively impact police morale. Observers believe this action would have a serious negative effect on the government's ability to investigate and prosecute money laundering and terrorist finance cases.

Despite these staffing challenges, an increase in the government's political will and attention to the problems of money laundering and financial crimes has slightly improved the results of law enforcement and prosecutorial efforts. Prior to 2004, the Czech Republic had not successfully prosecuted a money laundering case. However, in 2004 the Ministry of Justice achieved its first four convictions against individuals attempting to legalize the proceeds from crime. Unfortunately, sentences were very low and consisted of probation. In 2005, 23 alleged offenders were prosecuted and three were convicted. In the first six months of 2006, courts increased convictions to 5 individuals. However; only 6 people were prosecuted during the same time period, a marked decrease from the previous year. Sentences were again low including suspended sentences or fines. An ongoing issue in

criminal prosecutions is that law enforcement must prove that the assets in question were derived from criminal activity. The accused is not obligated to prove that the property or assets were acquired legitimately.

The number of suspicious transaction reports transmitted to the FAU in 2005 grew slightly after a significant jump in 2004. The number of inquiries evaluated and forwarded to law enforcement doubled in 2005. This trend is interpreted as evidence of the active participation of obliged entities in the anti-money laundering regime and police suspicion of financial activities of groups and individuals suspected of some cooperation with terrorism groups. There were 3,267 suspicious transactions reported in 2004, and 3,404 in 2005. From January through September 2006, there were 2,043 reports of suspicious transactions. The number of reports forwarded to the police in 2004 by the FAU was 103. This number rose significantly in 2005 to 208. From January through September 2006, the number of reports forwarded to the police was 102. Every case that was passed to law enforcement was investigated. In 2005, the FAU received 130 assistance requests from abroad and sent 69 requests abroad. During the first nine months of 2006, the FAU received 84 requests and sent out 69 requests. From January to October 2006, the Financial Police's Department of Criminal Proceeds and Money Laundering investigated 76 cases and seized assets valued at 1.42 billion crowns (approximately $64.6 million). This figure is a significant increase over 2005, when the Department investigated 99 cases and seized assets valued at roughly 931 million crowns (approximately $42.3 million) and a monumental upsurge when compared to 2004 when the Department investigated 139 cases and seized assets only valued around 2 million crowns (approximately $91,000). Regarding drug cases, the Department participated in 12 cases in 2005 investigated by the Czech National Drug Headquarters, and seized assets valued at 48 million crowns (approximately $2 million) including three cars. Although the National Drug Headquarters continues close cooperation with the Czech Financial Police, during the first half of 2006, the amount of successfully seized assets from two cases decreased significantly to 1.34 million crowns (approximately $61,000).

In October 2005, the Czech Parliament ratified the UN International Convention for the Suppression of the Financing of Terrorism. This was a major step in that it marked both the implementation of the recommendations from international bodies and the completion of the statutory and organizational reforms required to effectively confront this issue. The Czech Government approved the National Action Plan of the Fight against Terrorism for 2005-2007 in November 2005. This document covers topics ranging from police work and cooperation to protection of security interests, enhancement of security standards, and customs issues. One of the major priorities contained in the plan continues to be the fight against terrorist financing.

In November 2004, the Czech Government amended the Criminal Code and enacted new definitions for terrorist attacks and terrorist financing. A penalty of up to 15 years imprisonment can be imposed on those who support terrorists financially, materially or by other means. Also, in addition to reporting all suspicious transactions possibly linked to money laundering, obliged institutions are now required to report all transactions suspected of being tied to terrorist financing. Multilateral bodies generally agree that the Czech Republic currently possesses an adequate regulatory basis with which to combat money laundering and terrorist financing.

In general, Czech authorities have been reliable partners in the battle against terrorist financing. Although the terrorist finance threat in the Czech Republic is generally modest, there is reason to believe that there has recently been an increased possibility of terrorist support activities in the country, and officials have publicly discussed the discovery of small hawala networks remitting funds from the Czech Republic to other parts of the world. 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. A governmental body called the Clearinghouse, instituted in 2002, was established to streamline the collection of information from institutions in order to enhance cooperation and response

to a terrorist threat. The Clearinghouse meets only in necessary cases. 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. An amendment to the anti-money laundering law in 2000 requires financial institutions to freeze assets that belong to suspected terrorists and terrorist organizations on the UN 1267 Sanctions Committees consolidated list. To date, two suspect accounts have been identified in Czech financial institutions based on the information provided by the United States. The accounts have been frozen and contain $500,000.

Although Czech law authorizes officials to use asset forfeiture, it is a relatively new tool and that is not widely used. It was introduced into the criminal system in 2002 and allows judges, prosecutors, or the police (with the prosecutor's assent) to freeze an account or assets if evidence indicates that 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 have to 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 implemented provisions and responsibilities overseeing the administration and storage of seized property and appoints the police as responsible for the administration of seized assets as well.

A recent amendment of Czech Criminal Procedure Code and Penal Code came into force in July 2006, bringing several positive changes to asset forfeiture and seizure. The law, as newly 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 effectively seize assets gained in illicit activity previously shielded by family members. The law allows for the seizure of substitute asset values as well as asset values not belonging to the criminal and appoints the police as responsible for administration of seized assets.

The Czech Republic has signed memoranda of understanding (MOUs) on information exchange with 22 countries, including new agreements with Australia and Canada. The Czech Republic also has a formalized agreement with Europol since 2002. The FAU is a member of the Egmont Group, and is also authorized to cooperate and share information with all of its international counterparts, including those not part of the Egmont Group. The Czech Republic actively participates in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). Cooperation and information exchange with international counterparts or other international organizations has a foundation in Czech law.

The Czech Republic 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. The Czech Republic is also a party to the World Customs Organization's Convention on Mutual Administrative Assistance for the Prevention, Investigation and Repression of Customs Offenses as well as the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

The United States and the Czech Republic have a Mutual Legal Assistance Treaty (MLAT), which entered into force on May 7, 2000, as well as an extradition treaty that has been in effect since 1925. In May 2006, the United States and the Czech Republic signed a supplemental extradition treaty and a supplemental MLAT to implement the U.S.-EU Agreements on these subjects; but these instruments have not yet been ratified.

The Czech Republic has made progress in its efforts to strengthen its money laundering regime, as demonstrated by its ratification in 2005 of the UN International Convention on the Suppression of the Financing of Terrorism and its expanded capacity to enforce existing money laundering regulations despite the threat of future personnel shortages. However, further improvement is still needed. The

Czech Republic has to date made only incremental and limited progress in its law enforcement efforts. Prosecutions are still infrequent and penalties have been far too light to serve as an effective deterrent. Standards of proof remain extremely high and assets forfeiture has not yet become a standard tool used by prosecutors and judges, although the government has given law enforcement the tools for seizing illicit assets shielded by family members. Czech law enforcement and customs authorities should intensify efforts to monitor underground markets and informal remittance systems, such as hawala, used often used by the immigrant communities. Many of these underground systems are based on the misuse of trade. However, changes under discussion to disband the Financial Police are troubling. Doing so would have a negative impact on the government's ability to investigate and prosecute money laundering and terrorist finance cases. The Czech Republic should ratify the UN Convention against Transnational Organized Crime and UN Convention against Corruption.

Dominica

The Commonwealth of Dominica initially sought to attract offshore dollars by offering a wide range of offshore financial services, low fees and minimal government oversight. A rapid expansion of Dominica's offshore sector without proper supervision made it attractive to international criminals and vulnerable to official corruption. In response to international criticism, Dominica enacted legislation to address many of the deficiencies in its anti-money laundering regime. In September 2006, Dominica announced its intentions to revive its offshore sector through the creation and development of new products and conditions. This includes adjustments to Dominica's economic citizenship program to encourage investors to fund Dominican business projects in exchange for citizenship.

Dominica's financial sector includes one offshore and four domestic banks, 17 credit unions, approximately 11,452 international business companies (IBCs) (a significant increase from 1,435 in 2002), 19 insurance agencies, six money service businesses, one building and loan society, and three operational internet gaming companies (although reports indicate more internet gaming sites exist). There are no free trade zones in Dominica.

Under Dominica's economic citizenship program, individuals can purchase Dominican passports and, in the past, official name changes for approximately $75,000 for an individual and $100,000 for a family of up to four persons. Although not very active, Dominica's economic citizenship program is not adequately regulated. Individuals from the Middle East, the former Soviet Union, the Peoples' Republic of China and other foreign countries have become Dominican citizens and entered the United States via a third country without visas. Subjects of United States criminal investigations have been identified as exploiting Dominica's economic citizenship program in the past.

In June 2000, the Financial Action Task Force (FATF) placed Dominica on its Non-Cooperative Countries and Territories (NCCT) list. As a result, Dominica implemented and revised anti-money laundering reforms and was removed from the NCCT list in October 2002. One of the reforms created was an Offshore Financial Services Council (OFSC). The OFSC's mandate is to advise the Government of the Commonwealth of Dominica (GCOD) on policy issues relating to the offshore sector and to make recommendations with respect to applications by service providers for licenses.

The Eastern Caribbean Central Bank (ECCB) acts as the primary supervisor and regulator of onshore banks in Dominica. A December 2000 agreement between the OFSC and the ECCB places Dominica's offshore banks under the dual supervision of the ECCB and the GCOD Financial Services Unit (FSU). In compliance with the agreement, the ECCB assesses applications for offshore banking licenses, conducts due diligence checks on applicants, and provides a recommendation to the Minister of Finance. The ECCB also conducts on-site inspections for anti-money laundering compliance of onshore and offshore banks in Dominica. The ECCB is unable to share examination information directly with foreign regulators or law enforcement personnel. The Minister of Finance is required to seek advice from the ECCB before exercising his powers with respect to licensing and enforcement.

The Offshore Banking (Amendment) Act 2000 prohibits the opening of anonymous accounts, prohibits IBCs from direct or indirect ownership of an offshore bank, and requires disclosure of beneficial owners and prior authorization to changes in beneficial ownership of banks. All offshore banks are required to maintain a physical presence in Dominica and have available for review on-site books and records of transactions.

The International Business Companies (Amendment) 2000 requires bearer shares to be kept with a registered agent who is required to maintain a register with the names and addresses of beneficial owners. Additional amendments to the Act in September 2001 require previously issued bearer shares to be registered. IBCs are not required to have a physical presence, nor do they have to file annual financial reports. IBCs are restricted from conducting local business activities. The Act empowers the FSU to "perform regulatory, investigatory, and enforcement functions" over IBCs. The International Business Unit (IBU) of the Ministry of Finance supervises and regulates offshore entities and domestic insurance companies.

The Money Laundering Prevention Act (MLPA) of December 2000, as amended in July 2001, criminalizes the laundering of proceeds from any indictable offense. In addition, the law applies not only to narcotics-related money laundering, but also to the illicit proceeds of all criminal acts, whether committed in Dominica or elsewhere. The MLPA overrides secrecy provisions in other legislation and requires financial institutions to keep records of transactions for at least seven years. The MLPA requires a wide range of financial institutions and businesses, including any offshore institutions, to report suspicious transactions simultaneously to the Money Laundering Supervisory Authority (MLSA) and Dominica's financial intelligence unit (FIU). Additionally, financial institutions are required to report any transaction over $5,000. The MLPA also requires persons to report cross-border movements of currency that exceed $10,000 to the FIU.

The MLSA is authorized to inspect and supervise nonbank financial institutions and regulated businesses for compliance with the MLPA. The MLSA consists of five members: a former bank manager, the IBU manager, the Deputy Commissioner of Police, a senior state attorney and the Deputy Comptroller of Customs. The MLSA is also responsible for developing anti-money laundering policies, issuing guidance notes and conducting training. The May 2001 Money Laundering Prevention Regulations apply to all onshore and offshore financial institutions including banks, trusts, insurance companies, money transmitters, regulated businesses and securities companies. The regulations specify client identification requirements, record keeping, and suspicious transaction reporting procedures, and require compliance officers and training programs for financial institutions. The regulations require that the true identity of the beneficial interests in accounts be established, and mandate the verification of the nature of the business and the source of the funds of the account holders and beneficiaries. Reporting entities are protected by law. Anti-Money Laundering Guidance Notes, also issued in May 2001, provide further instructions for complying with the MLPA and provide examples of suspicious transactions to be reported.

The FIU was also established under the MLPA and became operational in August 2001. The FIU is comprised of two full time staff members: a director and a financial analyst/investigator. A police officer with training in financial investigations is also assigned to the FIU on an as-needed basis. The FIU analyzes suspicious transaction reports (STRs) and cross-border currency transactions, forwards appropriate information to the Director of Public Prosecutions, and liaisons with other jurisdictions on financial crimes cases. The FIU has access to the records of financial institutions and other government agencies, with the exception of the Inland Revenue Division. In 2005, the FIU received 19 STRs, which is a significant decrease from the 122 STRs received in 2004. The decline continued in 2006 with the FIU receiving only six STRs.

The MLPA provides for freezing of assets for seven days by the FIU, after which time a suspect must be charged with money laundering or the assets released. Under the Act No. 20 of 2000 and Act No. 3

of 2003, all assets that can be linked to any individual or legitimate business under investigation can be seized or forfeited, providing that the amount seized or forfeited does not exceed the total benefit gained by the subject from the crime committed. The court can order the confiscation of frozen assets. Pursuant to the MLPA, tangible confiscated assets such as vehicles or boats are forfeited to the GCOD. Intangible assets such as cash or bank accounts are split between the Forfeiture Fund and the Government Consolidated Fund by 80 and 20 percent, respectively. The total amount of nonterrorist related assets frozen, forfeited and/or seized in the past year was $55,481, up from zero the year before.

There are no known convictions on money laundering charges in Dominica. In 2006, a French national—under investigation since 2004 for misappropriation of funds from Guadeloupe nationals—was arrested for attempting to obtain a line of credit through fraudulent wire transfers. In 2005, a Haitian national was arrested for human trafficking and money laundering. The GCOD also filed criminal complaints and is working with the United States authorities on a case against St. Regis University for issuing fraudulent degrees and laundering the proceeds in an offshore bank

On June 5, 2003, Dominica enacted the Suppression of Financing of Terrorism Act, which criminalizes the financing of terrorism. The Act also provides authority to identify, freeze and seize terrorist assets, and to revoke the registration of charities providing resources to terrorists. The MLSA and the Office of the Attorney General supervise and examine financial institutions for compliance with counterterrorist financing laws and regulations. The GCOD circulates the United Nations 1267 Sanctions Committee list to financial institutions, but to date, no accounts associated with terrorists or terrorist entities have been found in Dominica. The GCOD has not taken any specific initiatives focused on alternative remittance systems.

In May 2000, a mutual legal assistance treaty between Dominica and the United States entered into force. The GCOD also has a tax information exchange agreement with the United States. The MLPA authorizes the FIU to exchange information with foreign counterparts. The Exchange of Information Act 2002 provides for information exchange between regulators.

Dominica is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force (CFATF). The FIU became a member of the Egmont Group in June 2003. Dominica is a party to the 1988 UN Drug Convention. The GOCD has neither signed nor ratified the UN Convention against Transnational Organized Crime or the UN Convention against Corruption. Dominica acceded to the UN International Convention for the Suppression of the Financing of Terrorism and to the Inter-American Convention against Terrorism in September 2004.

The Government of the Commonwealth of Dominica should fully implement and enforce the provisions of its legislation and provide additional resources for regulating offshore entities, particularly international business companies (IBCs). Dominica should continue to develop the FIU to enable it to fulfill its responsibilities and cooperate with foreign authorities. The GOCD should eliminate its program of economic citizenship.

Dominican Republic

The Dominican Republic is a major transit country for drug trafficking. 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 2003 collapse of the country's third largest bank, Banco Intercontinental (Baninter), is a significant example of the corruption and money laundering scandals that plague the financial sector. The Baninter case saw approximately $2.2 billion evaporate over the course of just a few years due to the fraudulent accounting schemes orchestrated by senior officials. The trial phase began in mid-2006, but remains mired in procedural delays that could jeopardize the entire case. The failure of Baninter and two other banks (Banco Mercantil and Bancredito) cost the Government of the Dominican Republic (GODR) in excess of $3 billion and severely destabilized the country's finances. Criminal prosecutions are underway in all three cases. 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 in order to improve banking supervision. Though legislative changes have been made, full implementation of IMF requirements lags.

The enactment of Act 17 of December 1995 (the 1995 Narcotics Law) made narcotics-related money laundering a criminal offense. To update its anti-money laundering legislation in line with international standards, the GODR passed Law No. 72-02 in 2002 to expand money laundering predicate offenses beyond illegal drug activity to include other serious crimes, such as illicit 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 further imposes financial penalties on institutions that engage in money laundering. The GODR is currently considering an amendment to this law that would add criminal penalties to perpetrators of financial crimes.

Under Decree No. 288-1996 of the Superintendence of Banks, banks, currency exchange houses and stockbrokers are required to know and identify their customers, keep records of transactions (five years), record currency transactions greater than $10,000, and file suspicious transactions reports (STRs). Law No. 72-02 enhances requirements for customer identification, record keeping of transactions, and reporting of STRs. Law 72-02 also extends reporting requirements to numerous other financial and nonfinancial sectors, including 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, fund 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. 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.

The Unidad de Inteligencia Financiera (UIF) was created in 1997 as the financial intelligence unit (FIU) of the Dominican Republic. The UIF, a department within the Superintendence of Banks, receives financial disclosures and STRs from reporting entities in the financial sector. In 2002, Law 72-02 created the Unidad de Análisis Financiero (Financial Analysis Unit, or UAF) as a second FIU 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.

According to the GODR, the UAF has replaced the UIF as the FIU of the Dominican Republic. However, the UAF began operating in May 2005, and the UIF has not ceased operations. Therefore, it appears that a duality of FIU functions continues to exist between these two units. For instance, financial reporting entities may report to either the UIF or the UAF, while nonfinancial reporting entities must report to the UAF. For 2006, the UAF received 229 STRs and 22,610 reports of currency transaction reports. The majority of the reports the UAF received were transferred from the UIF. 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 and the GODR has formally criminalized terrorist financing, as the criminalization of terrorist financing is now a requirement for all new members of the Egmont Group.

In 2005, two asset seizure laws were clarified by an executive order stating that the measures set forth in Law No. 78-03 prevail over those contained in Law No. 72-02. Law No. 78-03 permits the seizure, conservation and administration of assets which are the product or instrument of criminal acts pending judgment and sentencing. The 1995 Narcotics Law allows preventive seizures and criminal forfeiture of drug-related assets, and authorizes international cooperation in forfeiture cases.

While numerous narcotics-related investigations were initiated under the 1995 Narcotics Law, and substantial currency and other assets were confiscated, there have been only three successful money laundering prosecutions under this law. In August 2006, the Attorney General's office created a financial crimes unit to actively pursue financial crimes and money laundering investigations to aide in prosecutors' ability to obtain money laundering convictions.

The GODR continues to support U.S. Government efforts to identify and block terrorist-related funds. Although no assets were 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. The GODR has not enacted specific legislation that would criminalize the financing terrorism and provide reporting entities with a legal basis to carry out counterterrorism financing prevention programs.

According to U.S. law enforcement officials, cooperation between law enforcement agencies on drug cases, human trafficking, and extradition matters remains strong. In 2006, the GODR assisted U.S. law enforcement authorities to disrupt a drug-trafficking and money laundering ring transferring $2-3 million in illicit remittances to the Dominican Republic per month.

The United States continues to encourage the GODR to join a mutual legal assistance treaty with the Organization of American States (OAS) and sign related money laundering conventions. The Dominican Republic 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. The Dominican Republic is a party to the 1988 UN Drug Convention. The GODR has signed, but has not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism. On October 26, 2006, the GODR ratified the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. On August 10, 2006, the Dominican Republic became a party to the Inter-American Convention against Terrorism.

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, and ensure this sector's compliance with reporting requirements. The Dominican Republic should bolster the operational capacity of the fledgling UAF and ensure a full transition of FIU functions. The GODR should formally criminalize the financing of terrorism.

Ecuador

With a dollar economy geographically situated between two major drug producing countries, Ecuador is highly vulnerable to money laundering but is not considered an important regional financial center. Because thus far there has not been fully effective control of money laundering, 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. 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.

On October 18, 2005, Ecuador's new comprehensive law against money laundering was published in the country's Official Register. The new law, Law 2005-13, criminalizes the laundering of illicit funds from any source and penalizes the undeclared entry of more than $10,000 in cash or other convertible assets. The law calls for the creation of a financial intelligence unit (FIU) under the purview of the National Council Against Money Laundering. Regulations for application of the law and establishment of the FIU were published in April 2006. The FIU director was appointed in November 2006, and the hiring of personnel began in January 2007.

The National Council Against Money Laundering, established under Law 2005-13, is headed by the Procurador General (solicitor general) and includes representatives of all government entities involved in fighting money laundering, such as the Superintendence of Banks and the National Police. The National Council Against Money Laundering will be 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.

Ecuador's first major money laundering case broke 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. Accused drug trafficker Hernan Prada Cortes, recently extradited to the United States from Colombia, had acquired many Ecuadorian businesses and real properties in the names of other persons since 2000. Faced with the need to prosecute successfully this high-visibility case before the new FIU is in place, the GOE is making efforts to resolve pending issues.

Prior to the passage of the 2005 law, the Narcotics and Psychotropic Substance Act of 1990 (Law 108) criminalized money laundering activities only in connection with illicit drug trafficking. Under the new law, money laundering is criminalized in relation to any illegal activity, including narcotics trafficking, trafficking in persons and prostitution, among others. Money laundering is penalized by a prison term of three to nine years, depending upon the amount laundered, as well as a monetary fine.

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 FIU, once it is operational. Obligated entities are also required to report cash transactions exceeding $10,000, establish "know-your-client" provisions, and maintain financial transaction records for ten years. Any person entering or leaving Ecuador with $10,000 or more must file a report with the customs service. Entities or persons who fail to file the required reports or declarations may be sanctioned by the Superintendence of Banks. The FIU 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 Public Ministry. The FIU is also empowered to exchange information with other financial intelligence units on the basis of reciprocity.

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 Superintendence of Banks. In addition, the Criminal Defamation Law sanctions banks and other financial institutions that provide information about accounts to police or advise the police of suspicious transactions if no criminal activity is proven. These obstacles can be overcome by a judge properly issuing an appropriate warrant. However, as a result of this contradictory legal framework, cooperation between other Government of Ecuador

(GOE) agencies and the police has in the past fallen short of the level needed for effective enforcement of money laundering statutes.

Several Ecuadorian banks maintain offshore offices. The Superintendence of Banks 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 Superintendence of Banks. These private accounting firms perform the standard audits on offshore banks that would generally be undertaken by the Superintendence in Ecuador. Bearer shares are not permitted for banks or companies in Ecuador.

A free trade zone law was passed in 1991 in order to promote exports, foreign investment, and employment. The law provides for the import of raw materials and machinery free of duty and tax; the export of finished and semi-processed goods free of duty and tax; and tax exemptions for business activities in the government-established zones. Free trade zones have been established in Esmeraldas, Manabi and Pichincha provinces, and a new zone is planned for the site of the new Quito airport. There is no known evidence to indicate that the free trade zones are being used in trade-based money laundering.

Terrorist financing has not been criminalized in Ecuador. The Ministry of Foreign Affairs, Superintendence of Banks and the Association of Private Banks formed a working group in December 2004 to draft a law against terrorist financing. By year-end 2006, the draft law had passed its first debate in Congress. The Superintendence 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 Superintendence would have to obtain a court order to freeze or seize such assets, in the event they were identified in Ecuador. No steps have been taken to prevent the use of gold and precious metals to launder terrorist assets. Currently, there are no measures in place to prevent the misuse of charitable or nonprofit entities to finance terrorist activities.

Ecuador 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 Transnational Organized Crime and the UN Convention against Corruption. On July 27, 2006, the Government of Ecuador (GOE) ratified the Inter-American Convention against Terrorism. Ecuador is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering and the Financial Action Task Force of South America (GAFISUD). The GOE is scheduled to undergo a mutual evaluation by GAFISUD in 2007. 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 an Agreement to Implement the United Nations Convention against Illicit Trafficking in Narcotic Drugs and Psychotropic Substances of December 1988, 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 U.S. to share information on currency transactions.

Ecuador is one of only two countries in South America that is not a member of the Egmont Group of financial intelligence units. Now that the necessary legislative framework exists, the GOE should quickly establish a fully functioning FIU that meets the standards of the Egmont Group and the Financial Action Task Force. Ecuador should criminalize the financing of terrorism, which is a prerequisite for membership in the Egmont Group and is necessary in order to fully comply with international anti-money laundering and counterterrorist financing standards. The GOE should also

address items that were not accounted for in the new money laundering legislation, including the abolition of strict bank secrecy limitations and any potential sanctions for financial institutions that report suspicious transactions.

Egypt, The Arab Republic of

Egypt is not considered a regional financial center or a major money laundering country. The Government of Egypt (GOE) continued financial sector reform in 2006, privatizing the Bank of Alexandria (BOA), the smallest of the four public banks, which was sold to Italy's Sanpaolo IMI. The GOE also undertook initiatives to improve stock market regulation and transparency, stimulate the mortgage sector, reform Central Bank management and restructure public insurance companies. Despite these reforms, Egypt still has a large, informal cash economy, and many financial transactions do not enter the banking system at all. Of the few money laundering cases that have made it to court in the last several years, most involved illegal dealings in antiquities and misappropriation of public funds.

While there is no significant market for illicit or smuggled goods in Egypt, there is evidence that arms are being smuggled across Egypt's border with Gaza. The funding source is unclear, as is the destination of the proceeds. Other than arms, authorities say that 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. Customs fraud and invoice manipulation are also found in regional value transfer and countervaluation in hawala transactions. The Ministry of Finance has indicated that more businesses and individuals are filing tax returns as a result of June 2005 tax cuts. Nevertheless, a large portion of Egypt's economy remains undocumented.

At present, money laundering and terrorist financing are not reported to be widespread. Most cases of money laundering that have been detected have involved laundering of money through the formal banking sector. Informal remittance systems are unregulated and therefore pose a potential means for laundering funds. Egyptian authorities claim that informal remittances are not widespread in Egypt, but the number of remittances officially recorded by banks does not match the large number of Egyptians working overseas, in the Gulf and elsewhere. Reports on the number of Egyptian expatriates are contradictory, but the figure generally stated is 5 million. One report claimed that these expatriates transfer remittances amounting to $5 billion annually: $3.3 billion transmitted through official means (i.e., banks, Western Union); and $1.5 billion through informal means. Many overseas workers use informal means due to a lack of trust in or familiarity with banking procedures or the lower costs associated with informal remittance systems. Due to the unregulated nature of informal remittance systems, it is unclear if and to what extent money laundering actually occurs through these systems. Western Union, the only formal cash transfer operator in Egypt, continues to draw customers.

Egypt does not have a high prevalence of financial crimes, such as counterfeiting or bank fraud. There is no evidence that Egyptian institutions engage in currency transactions involving international narcotics trafficking proceeds. 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. The law did not repeal Egypt's existing law on bank secrecy, but it did provide 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 Central Bank of Egypt (CBE). The administrative regulations of the anti-money laundering (AML) law provide the legal basis by which the MLCU derives its authority, spelled out the predicate crimes associated with money laundering, established a Council of Trustees to govern the MLCU, defined the role of supervisory authorities and financial institutions, and allowed

for the exchange of information with foreign competent authorities. Article 86 of the Penal Code criminalizes the financing of terrorism.

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 large transactions. In addition, banks are required to submit quarterly reports showing compliance with respect to their AML responsibilities. Reporting of suspicious transactions is voluntary by banks and nonbank financial institutions.

In 2006, the CBE and MLCU undertook special compliance assessments of all banks operating in Egypt. The assessments consisted of questionnaires and on-site visits to check AML systems in place in banks. Based on the assessments, banks were divided into three categories: fully compliant, partially compliant, and noncompliant. To date, only one bank has been found noncompliant. Where deficiencies were found, banks were notified of corrective measures to be undertaken with a deadline for making the necessary changes and follow-up visits to reassess compliance. 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. CBE and MLCU officials have indicated that they will continue to conduct comprehensive periodic assessments of all banks.

The CBE also monitors bureaux de change and money transmission companies for foreign exchange control purposes, giving special attention to those accounts with transactions above certain limits. The Capital Market Authority (CMA), which is responsible for regulating the securities markets, has also undertaken the inspection of firms and independent brokers and dealers under its jurisdiction. The inspections were 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.

In 2006, an independent insurance regulatory authority was established and charged with supervising insurance companies 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, accountants, and cash couriers, are not currently subject to AML controls, although MLCU officials have indicated that the law will soon be amended to cover the activities of these individuals. The AML law protects institutions and individuals who cooperate with law enforcement officials.

The executive regulations of the AML law lowered the threshold for declaring foreign currency at borders from the equivalent of $20,000 to $10,000. The declaration requirement was also extended to travelers leaving as well as entering the country. Enforcement of this provision is not consistent, however. The Customs Authority also signed an agreement with the MLCU to share information on currency declarations. Further impetus to law enforcement was added on account of reports that Hamas ministers from the Palestinian Authority were crossing the Egypt-Gaza border with large amounts of cash. Egyptian Customs Authorities now 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 claim that the 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 11 public free zones, several private free zones, and one SEZ, though more of the latter may be opened soon. 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. Activity in the free zones and SEZs is not subject to Egypt's anti-money laundering law (AML), but there is no indication that the zones are being used for trade-based money laundering schemes or for financing of terrorism.

The MLCU, Egypt's FIU, is an independent entity within the CBE. The MLCU has its own budget and staff, and also has the full legal authority to examine all Suspicious Transaction Reports (STRs) and conduct investigations. Investigations are conducted with the assistance of counterpart law enforcement agencies, including the Ministry of Interior, the National Security Agency, and the Administrative Control Authority. The MLCU shares information with all of these agencies. The unit handles implementation of the AML law, which includes publishing the executive directives. The MLCU takes its direction from a six-member council, which is chaired by the Assistant Minister of Justice for Legislative Affairs. Other members of the council include the Chairman of the CMA, the Deputy Governor of the CBE, a Sub-Minister from the Ministry of Social Solidarity, 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 of FIUs. MLCU has received extensive training by U.S., European, and Australian anti-money laundering and counterterrorist financing authorities.

The Executive Director of the MLCU is responsible for the operation of the FIU and the implementation of the policies drafted by the Council of Trustees. His responsibilities include: proposing procedures and rules to be observed by different entities involved in combating money laundering; presenting these rules and procedures to the Chairman of the Council of Trustees; reviewing the regulations issued by supervisory authorities for consistency with legal obligations and ensuring that they are up to date; ensuring the capability and readiness of the unit's database; exchanging information with supervisory entities abroad; acting as a point of contact within the GOE; preparing periodic and annual reports on the operational status of the unit; and taking necessary action on STRs recommended to be reported to the Office of Public Prosecution.

Since its inception in 2003, the MLCU has received several thousand STRs from financial institutions and has successfully brought several cases to court. 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 AML department works closely with the MLCU during investigations. It has established its own database to record all the information it 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 GOE established a national committee for coordinating issues regarding anti-money laundering in late 2005.

In 2002, the GOE passed the Law on Civil Associations and Establishments (Law No. 84 of 2002), which 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. Both the Ministry of Social Solidarity and the CBE continually monitor 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 authorizes seizure 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.

Because of its own historical problems with domestic terrorism, the GOE has sought closer international cooperation to counter terrorism and terrorist financing. The GOE has shown a willingness to cooperate with foreign authorities in criminal investigations, whether they are related to terrorism or narcotics.

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, and the National Security Agency, in addition to the MCLU. The same agencies sit on a National Committee for International Cooperation in Combating Terrorism, which was established in 1998.

The GOE is in the process of replacing its original counterterrorism law, an emergency law enacted in 1981, with a new and updated law. It will reportedly include specific measures against terrorist financing.

The United States and Egypt 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 UK, Romania, Zimbabwe and Peru. The CBE circulates to all financial institutions the 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 Executive Order 13224. No related assets were identified, frozen, seized, or forfeited in 2006.

Egypt is a founding member of the Middle East and North Africa Financial Action Task Force (MENAFATF) and follows that organization's recommendations on anti-money laundering and counterterrorist financing. In January 2006, Egypt assumed the presidency of MENAFATF for a one-year period. Egypt is a party to the 1988 UN Drug Convention. In March 2004, it ratified the UN Convention against Transnational Organized Crime. In March 2005, it ratified the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Egypt should follow through with its plans to enact an updated law against terrorism that specifically addresses the threat of terrorist financing, including asset identification, seizure and forfeiture. The GOE must also improve its ability to pursue suspicious financial activities and transactions through the entire investigative and judicial process. Egypt should work to increase the number of successful money laundering investigations, prosecutions, and convictions. It 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, regardless of whether couriers have followed required

reporting procedures. Egyptian authorities should investigate underground value transfer systems and their possible relationship with money laundering and terrorist finance.

El Salvador

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. Its most significant financial contacts are with neighboring Central American countries, as well as with the United States, Mexico and the Dominican Republic. 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. In 2006, approximately $3.3 billion in remittances were sent to El Salvador through the financial system. Most were sent from Salvadorans working in the United States to family members. The quantity of additional remittances that flow back to El Salvador via other methods such as visiting relatives, regular mail and alternative remittance systems is not known.

Most money laundering is conducted by international criminal organizations. These organizations use bank and wire fund 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 1998, the "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 establishes the financial intelligence unit (FIU), the Unidad de Inteligencia Financiera (UIF), within the Attorney General's Office. The UIF 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 UIF. 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.

Cooperation between the Attorney General's Office and the police has resulted in the conviction of two individuals for money laundering offenses, and the arrests of several high-profile individuals suspected of money laundering and other financial crimes. Additionally, the Government of El Salvador (GOES) has recently begun to investigate private companies and financial service providers involved in suspicious financial activities. Despite demonstrating a greater commitment to pursue financial crimes over the previous year, 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 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 investigations. The system became operational in the last quarter of the year and is expected to greatly enhance investigative capabilities.

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 it. In 2006, the PNC seized over $2.2 million in undeclared cash from individuals transiting El Salvador's international airport and land border crossings.

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, the process does not often result in the forfeiture of funds that are then channeled to counternarcotics operations. There exists no legal mechanism to share seized assets with other countries. Salvadoran law currently provides only for the judicial forfeiture of assets upon conviction (criminal forfeiture), and not for civil or administrative forfeiture. A draft law to reform Decree 498 to provide for civil forfeiture of assets has stalled in the national legislature.

The GOES passed counterterrorism legislation, Decree No. 108, on September 19, 2006. Decree No. 108 further defines acts of terrorism and establishes tougher penalties for the execution of those acts. Article 29 of Decree No. 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) that were included in an early draft were not included in the final law.

The GOES has circulated the names of suspected terrorists and terrorist organizations listed on the 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 UIF to sign agreements in order to share or provide information to other countries. The GOES is party to the Organization of American States (OAS) Inter-American Convention on Mutual Assistance in Criminal Matters, which provides for parties to cooperate in tracking and seizing assets. The UIF 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, terrorism 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. The UIF has been a member of the Egmont Group since 2000. The GOES is party to the OAS Inter-

American Convention against Terrorism, the UN International 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 is also a signatory to the Central American Convention for the Prevention and Repression of Money Laundering Crimes Related to Illicit Drug Trafficking and Related Crimes.

The Government of El Salvador made advances in 2006 with the passage of counterterrorist financing legislation. El Salvador should continue to expand and enhance its anti-money laundering policies and strengthen its ability to seize and share assets. Remittances are an important sector of the economy, which must therefore be carefully supervised. The GOES should improve supervision of cash couriers and wire transfers as outlined in the Financial Action Task Force (FATF) Special Recommendations on terrorism financing. The GOES should also ensure that sufficient resources are provided to the overburdened Attorney General's office and the financial and narcotics divisions of the police.

France

France remains an attractive venue for money laundering because of its sizable economy, political stability, and sophisticated financial system. However, France has put in place comprehensive financial controls, and it is an active partner in international efforts to control money laundering and the financing of terrorism.

The Government of France (GOF) first criminalized money laundering related to narcotics trafficking in 1987. In 1988, the Customs Code was amended to incorporate financial dealings with money launderers as a crime and in May 1996 the criminalization of money laundering was expanded to cover the proceeds of all crimes with Law No. 96-392. 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.

Article 324-1 of the Penal Code provides that money laundering is punishable by five years imprisonment and a fine of 375,000 euro (approximately $481,000). With aggravating circumstances such as habitual or organized activity (Article 324-2) or connection with narcotics trafficking (Article 222-38), the punishment increases to ten years imprisonment and a fine of 750,000 euro (approximately $962,000). In 1990, the obligation for financial institutions to combat money laundering came into effect with the adoption of the anti-money laundering (AML) law—now incorporated in the Monetary and Financial Code (MFC) and France's ratification of the 1988 UN Drug Convention. Suspicious transaction reporting is now required for a wide variety of financial and nonfinancial entities, including banks, insurance companies, casinos, and lawyers.

As a member of the European Union (EU), France is obligated to implement all three EU money laundering directives, including Directive 2001/97/EC, which was transposed into domestic French legislation in 2004. With Decree 2006-736 of 26 June 2006, France incorporated the EU's Second Money Laundering Directive into French law. The EU adopted the Third Money Laundering Directive (2005/60/EC) in late 2005, which must be implemented in France by December 15, 2007.

Decree No. 2002-770 of 2002 addresses the functions of France's Liaison Committee against the Laundering of the Proceeds of Crime. This committee is co-chaired by the French financial intelligence unit (FIU), known as the unit for Treatment of Intelligence and Action Against Clandestine Financial Circuits or TRACFIN, and the Justice Ministry. It comprises 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 anti-money laundering system.

The Banking Commission supervises financial institutions and conducts regular audits of credit institutions. The Insurance and Provident Institutions Supervision Commission reviews insurance brokers. The Financial Market Authority, which evolved from the merger of the Securities Exchange Commission and the Financial Markets Council, monitors the reporting compliance of the stock exchange and other nonbank financial institutions. The Central Bank (Banque de France) oversees management of the required records to monitor banking transactions, such as those for means of payment (checks and ATM cards) or extensions of credit. Bank regulators and law enforcement can access the system managed by the French Tax Administration for opening and closing of accounts, which covers depository accounts, transferable securities, and other properties including cash assets that are registered in France. These records are important tools in the French arsenal for combating money laundering and terrorism financing.

TRACFIN is responsible for analyzing suspicious transaction reports (STRs) filed by French financial institutions and nonfinancial professions. TRACFIN participates in FINATER, an informal group created within the French Ministry of the Economy, Finance, and Industry in September 2001 to gather information to fight terrorist financing. 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. With the Law of 15 May 2001, 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 10,842 STRs in 2004, 11,553 in 2005 and 12,047 in 2006. Approximately 83 percent of STRs are sent from the banking sector. A total of 308 cases were referred to the judicial authorities in 2003, which resulted in 63 convictions. The FIU referred 347 cases in 2004, 405 in 2005 and 411 in 2006.

In addition to STRs, two other types of reports are required to be filed with the FIU. First, a report must be filed with TRACFIN when the identity of the principal or beneficiary remains doubtful despite due diligence; there is no threshold limit for such reporting. Second, a report must be filed in cases where transactions are carried out on behalf of a third party natural person or legal entity (including their subsidiaries or establishments) by a financial entity acting in the form, or on behalf, of a trust fund or any other asset management instrument, when legal or beneficial owners are not known. 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 the Financial Action Task Force (FATF) list of noncooperative countries or territories.

Laws No. 98-546 and 2001-420, of July 1998 and May 2001 respectively, extended the reporting obligations to new businesses. In addition, the laws ensured that with regard to criminal law, legal proceedings for "criminal conspiracy" are applicable to money laundering. While Law No. 96-392 of 1996 instituted procedures for seizure and confiscation of the proceeds of crime, these laws permit seizure of all or part of property.

Since 1986, French counterterrorism legislation has provided for the prosecution of those involved in the financing of terrorism under the more severe offense of complicity in the act of terrorism. However, in order to strengthen this provision, the Act of November 15, 2001, introduced several new characterizations of offenses, specifically including the financing of terrorism. The offense of financing terrorist activities (Article 421-2-2 of the Penal Code) is defined according to the UN International Convention for the Suppression of the Financing of Terrorism and can result in ten years' imprisonment and a fine of 225,000 euro (about $289,000). Since 2001, TRACFIN has referred 92 cases of suspected terrorist financing to the judicial authorities for prosecution. An additional penalty

of confiscation of the total assets of the terrorist offender has also been implemented. Accounts and financial assets can be frozen through both administrative and judicial measures.

In 2006, the GOF moved to strengthen France's antiterrorism legal arsenal with the Act of 23 January 2006, authorizing video surveillance of public places, including nuclear and industrial sites, airports, and railway stations. The Act requires telephone operators and Internet café owners to keep extensive records, allows greater government access to e-communications, and allows flight passenger lists and identification information to become accessible to counterterrorism officials. It stiffens prison sentences for directing a terrorist enterprise to 30 years and extends the possible period of detention without charge. The Act permits increased surveillance of potential targets of terrorism. It 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, or to companies directly or indirectly controlled by these individuals. By granting explicit national authority to freeze assets, the Act plugs up a potential loophole concerning the freezing of citizen versus resident EU-member assets. Adopted in January 2006, it was expected to enter into force by presidential decree before the end of 2006.

French authorities moved rapidly to freeze financial assets of organizations associated with al-Qaida and the Taliban under United Nations Security Council Resolution 1267. France takes actions against other terrorist groups through the EU-wide "clearinghouse" procedure. Within the Group of Eight, which it chaired in 2003, France has sought to support and expand efforts targeting terrorist financing. Bilaterally, France has worked to improve the capabilities of its African partners in targeting terrorist financing by offering technical assistance. On the operational level, French law enforcement cooperation targeting terrorist financing continues to be strong.

The United States and France have entered into a mutual legal assistance treaty (MLAT), which came into force 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 30 foreign FIUs.

France is a member of the FATF and held the FATF Presidency for a one-year term during 2004-05. 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). France is a party to the 1988 UN Drug Convention; the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime; the UN Convention against Transnational Organized Crime; the UN International Convention for the Suppression of the Financing of Terrorism; and the UN Convention against Corruption.

The Government of France has established a comprehensive anti-money laundering regime. France should continue its active participation in international organizations to combat the domestic and global threats of money laundering and terrorist financing.

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. Both the domestic consumption and the transiting of narcotics are additional sources of money laundering in Germany. According to the German Financial Intelligence Unit's (FIU's) annual report, about three-fourths of the suspicious transaction reports (STRs) filed in Germany cite suspected fraud, forgery and tax evasion. Germany is not an offshore financial center.

In 2002, the German Government (GOG) enacted a number of laws to improve authorities' ability to combat money laundering and terrorist financing. The 2002 measures brought German laws into line with the first and second European Union (EU) Money Laundering Directives, which mandate suspicious activity reporting by a variety of entities, including notaries, accountants, tax consultants, casinos, luxury item retailers, and attorneys.

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 $19,520). 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 FIU located within the Federal Office of Criminal Investigation (Bundeskriminalamt or BKA), as well as to the State Attorney (Staatsanwaltschaft).

The GOG has directed the Interior Ministry to draft new legislation to implement the third EU Money Laundering Directive by December 2007. In addition to requiring that EU member states implement the Financial Action Task Force's (FATF) Forty Recommendations, the directive contains further provisions on customer due diligence and other internal risk-management measures to prevent money laundering. The directive calls for improved integrity and transparency to help prevent financial crime and improve information exchange between the public and private sectors. The EU requirement also expands reporting requirements to encompass transactions which support the financing of terrorism or would do so if actually effected.

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 compile a centralized register of all bank accounts in Germany, including 300 million deposit accounts. As a result, in 2003 BaFIN established a central database with electronic access to all key account data held by banks in Germany. Banks cooperate with authorities and use computer-aided systems to analyze customers and their financial dealings to identify suspicious activity. Many of Germany's banks have independently developed risk assessment software to screen potential and existing clients and to monitor transactions for suspicious activity.

In 2002, Germany established a single, centralized, federal FIU within the BKA. Staffed with financial market supervision, customs, and legal experts, the FIU is responsible for developing a central database to use when analyzing cases and responding to reports of suspicious transactions. Another unit under the BKA, the Federal Financial Crimes Investigation Task Force, houses twenty BKA officers and customs agents.

In 2005, obligated entities submitted more than 8,000 STRs to the FIU. Approximately forty-five percent of the persons cited in German STRs are non-German nationals. Eighty-five percent of the reports resulted in investigative action. As with other crimes, actual enforcement under the German federal system is carried out at the state (sub-federal) level. Each state has a joint customs/police/financial investigations unit (GFG), which works closely with the federal FIU. In 2004, that the most recent year for which data is available, there were 109 money laundering convictions. The State Attorney can order a freeze of accounts when warranted.

As an EU member, Germany complies with a recent EU regulation requiring accurate originator information on funds transfers—but only for transfers into or out of the EU, not within the EU. FATF Special Recommendation Seven on Terrorist Financing, which governs wire transfers, however, requires such information on all cross-border transfers, including transfers between EU members.

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. The first reform package closed loopholes that had permitted members of foreign terrorist organizations to engage in fundraising in Germany (e.g., through charitable organizations) that extremists had exploited to advocate violence. Subsequently, Germany increased its law enforcement efforts to prevent misuse of charitable entities. Germany has used its Law on Associations (Vereinsgesetz) to take administrative action to ban extremist associations that "threaten the democratic constitutional order."

The second reform package, which went into effect January 1, 2002, 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. Another proposed counterterrorism reform, will further streamline and simplify security agencies' access to German financial, travel, and telephone records. In 2002, the GOG also added terrorism and terrorist financing to its list predicate offenses for money laundering, as defined by Section 261 of the Federal Criminal Code. A 2002 amendment of the Criminal Code allows prosecution of members of terrorist organizations based outside Germany

An immigration law, effective January 2005, contains provisions designed to facilitate the deportation of foreigners who support terrorist organizations.

A November 2003 amendment to the Banking Act created a broad legal basis for BaFIN to order freezes of assets of suspected terrorists who are EU residents, although authorities concentrate on financial assets. While BaFIN's system allows for immediate identification of financial assets for potential freezes and German law enforcement authorities can freeze accounts for up to nine months, money cannot be seized until authorities prove in court that the funds were derived from criminal activity or intended for terrorist activity. Sanctions imposed by the United Nations Security Council (UNSC) are exempted from the rule.

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 German financial institutions. In 2005, authorities found and froze less than 20,000 euros (approximately $26,000) in connection with names appearing on the 1267 consolidated list. A court can order the freezing of nonfinancial assets, but Germany typically does not do so, even when the action is pursuant to EU or UNSCR 1267 listings. Germany and several other EU member states have 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 Clearinghouse process.

Proceeds from asset seizures and forfeitures are paid into the federal government treasury. German authorities cooperate with U.S. authorities to trace and seize assets to the full extent allowed under German laws. German law does not allow for sharing forfeited assets with other countries.

Since 1998, the GOG has licensed and supervised money transmitters, shut down thousands of unlicensed money remitters, and issued anti-money laundering guidelines to the industry. A 1998 German law requires individuals to declare when they are entering, departing, or transiting the country with over 15,000 euros (approximately $19,400). A new European Union (EU) law, applicable to all EU members, is expected to take effect in June 2007 and will lower this amount to 10,000 euros (approximately $13,000)

Germany 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. BaFIN has investigated more than 2,500 cases of unauthorized financial services since 2003. It closed down more than 200 informal financial networks in 2005. There are currently 52 legally licensed money transfer services in Germany.

Germany exchanges law enforcement information with the United States through bilateral law enforcement agreements and informal mechanisms. United States and German authorities have conducted joint investigations. German law enforcement authorities cooperate closely at the EU level, such as through Europol. Germany has Mutual Legal Assistance Treaties (MLATs) with numerous countries. The MLAT with the United States was signed in October 2003. On July 27, 2006, the U.S. Senate ratified the MLAT; once the German parliament ratifies it, the two sides will exchange letters to bring the MLAT into force. In addition, the U.S.-EU Agreements on Mutual Legal Assistance and Extradition are expected to further improve U.S.-German legal cooperation.

Germany is a member of the FATF, the EU and the Council of Europe. Its FIU is a member of the Egmont Group. Germany is party to the 1988 UN Drug Convention, the UN International 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 anti-money laundering laws and its ratification of international instruments underline Germany's continued efforts to combat money laundering and terrorist finance. 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 Clearinghouse for financial crime and terrorism financing, so that the freezing process does not require a criminal investigation. German legislation should be amended to allow asset sharing with other countries. Germany should ratify the UN Convention against Corruption.

Gibraltar

Gibraltar is a largely self-governing overseas territory of the United Kingdom (UK), which assumes responsibility for Gibraltar's defense and international affairs. As part of the European Union (EU), Gibraltar is required to implement all relevant EU directives, including those relating to anti-money laundering.

The Drug Offenses Ordinance (DOO) of 1995 and Criminal Justice Ordinance to Combat Money Laundering criminalize money laundering related to all crimes. These ordinances also mandate suspicious transaction reporting for the financial sector and for designated nonfinancial businesses, which include 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. Obliged entities must submit suspicious transactions reports (STRs) to Gibraltar's financial intelligence unit (FIU).

The Financial Services Commission (FSC) regulates and supervises Gibraltar's financial services industry. Because of statutory requirements, the FSC must match the supervisory standards set by the UK. The FSC issues comprehensive AML Guidance Notes, which have the force of law, to clarify the obligations of Gibraltar's financial service providers. Financial institutions must retain records for at least five years from the date of the most recent transaction. If the obligated institution has submitted an STR to the FIU, or when a client or transaction is under investigation, it must maintain any relevant record even if the five year mandate has expired. Offshore banks are subject to the same legal and supervisory requirements as onshore.

The FSC also licenses and regulates the activities of trust and company management services, insurance companies, and collective investment schemes. The Government of Gibraltar (GOG)

permits internet gaming, and maintains a licensing regime for that sector. Gibraltar has circulated guidelines for correspondent banking, politically exposed persons, bearer securities, and "know your customer" (KYC) procedures.

The 2001 "Terrorism (United Nations Measures) (Overseas Territories) Order" criminalizes terrorism financing. Under this Order, if a financial institution suspects or knows that a customer is a terrorist or is linked to terrorism, including terrorist financing, the institution must report that customer.

In 1996, Gibraltar established the Gibraltar Coordinating Center for Criminal Intelligence and Drugs (GCID) as a sub-unit of the Gibraltar Criminal Intelligence Department. The GCID serves as Gibraltar's FIU. As such, it serves as the central point for receiving both financial and terrorism-related disclosures and receives, analyzes, and disseminates STR information filed by obliged institutions, The GCID is staffed mainly with police and customs officers, but is independent of any law enforcement agency. The FIU received 108 STRs in 2005, and 118 in 2006. There is a confiscation regime in place, but in order to confiscate assets in a money laundering case, the law enforcement agency investigating the case must be able to link the funds passing through the financial system with the original illicit funds. If this link cannot be substantiated, the funds cannot be confiscated.

The United Kingdom has not extended the Mutual Legal Assistance Treaty between itself and the United States to Gibraltar. However, a 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 the EU and Council of Europe partners. The GOG has implemented the 1988 UN Drug Convention pursuant to its Schengen obligations, but the UK has not extended the Convention to Gibraltar. Gibraltar is a member of the Offshore Group of Banking Supervisors (OGBS), and, in 2004, the GCID became a member of the Egmont Group.

The Government of Gibraltar should continue its efforts to implement a comprehensive anti-money laundering regime capable of thwarting terrorist financing. Gibraltar should put in place reporting requirements for cross-border currency movements. The GOG should pass legislation implementing the Financial Action Task Force's Nine Special Recommendations on Terrorist Financing. Gibraltar should also institute a regulatory scheme for its internet gaming sector in addition to its licensing regime. The GOG should work to implement the standards in the UN Convention against Corruption, the UN Convention against Transnational Organized Crime, and the UN Convention for the Suppression of the Financing of Terrorism.

Greece

While not a major financial center, Greece is fast becoming a regional financial center in the rapidly developing Balkans. Money laundering in Greece, due to the extensive use of currency in Greek society, is inherently difficult to detect. U.S. law enforcement agencies believe that criminally derived funds are typically not laundered through the banking system; rather they are most commonly invested in real estate, the lottery and a growing stock market. U.S. law enforcement agencies also believe Greece's location has led to a moderate increase in cross-border movements of illicit currency and monetary instruments due to the increasing interconnection of various financial services companies operating in Southeastern Europe and the Balkans. Reportedly, currency transactions involving international narcotics trafficking proceeds are not thought to include significant amounts of U.S. currency.

Greek authorities maintain that Greece is not an offshore financial center, and that there are no offshore financial institutions or international business companies (IBCs) per se operating within the country. However, Greek law (89/1967) provides for the establishment of companies which may be based in Greece but operate solely abroad. These firms are effectively excluded from supervision by Greece's tax authorities as they do not file taxes in Greece. "Law 89" companies, as they are known, mainly operate or claim to operate in the shipping industry and are known for their complex corporate and ownership structures. These firms fall under the authority of non-Greek jurisdictions and often operate through a large number of intermediaries. They could serve as a catalyst for money laundering. Although Greek law allows banking authorities to check these companies' transactions, such audits must be executed in conjunction with other Greek jurisdictions to be effective.

Greek law does not provide for nominee directors or trustees in Greek companies. Bearer shares have been abolished for banks and for a limited number of other companies, but most companies may issue bearer shares. Greece has three free trade zones, located at the ports of Piraeus, Thessalonica, and Heraklion, where foreign goods may be brought in without payment of customs duties or other taxes if they are subsequently transshipped or re-exported. Reportedly there is no indication that these zones are being used in trade-based money laundering or in the financing of terrorism.

The GOG criminalized money laundering derived from all crimes with the 1995 Law 2331/1995, entitled "Prevention of and Combating the Legalization of Income Derived from Criminal Activities." That law imposes a penalty for money laundering of up to ten years in prison and confiscation of the criminally-derived assets. The law also requires that banks and nonbank financial institutions file suspicious transaction reports (STRs) with Greece's financial intelligence unit (FIU). Legislation passed in March 2001 targets organized crime by making money laundering a criminal offense when the property holdings laundered are obtained through criminal activity or cooperation in criminal activity.

In November 2005, the GOG enacted Law 3424/2005, which extends the list of predicate offenses for money laundering to include terrorist financing, trafficking in persons, electronic fraud, and stock market manipulation. It also extends the STR reporting requirements to obligate additional sectors such as auction dealers and accountants. It furthermore broadens the powers of the supervisory authorities and clarifies previous legislation by ending a conflict between confidentiality rules and anti-money laundering regulations imposed on banks and other financial institutions. The law also provides supervisory authorities with greater authority to block transactions where money laundering is suspected and authorizes the FIU director to issue a temporary freeze of assets without the issuance of a court order. Through its Act 2577 9/2006, the Bank of Greece has applied the main provisions of the Third European Union (EU) Directive to all financial institutions. The GOG anticipates that the Directive will be formally transposed into national law in early 2008.

In 2003, Greece enacted legislation (Law 3148) that incorporates EU provisions in directives dealing with the operation of credit institutions and the operation and supervision of electronic money transfers. Under this legislation, the Bank of Greece has direct scrutiny and control over transactions by credit institutions and entities involved in providing services for fund transfers. The Bank of Greece issues operating licenses after a thorough check of the institutions, their management, and their capacity to ensure the transparency of transactions.

The Bank of Greece, through its Banking Supervision Department; the Ministry of National Economy and Finance, through its Capital Market Commission; and the Ministry of Development, through its Directorate of Insurance Companies, supervise and monitor credit and financial institutions. Supervision includes the issuance of guidelines and circulars, as well as on-site audits that incorporate a component assessing compliance with anti-money laundering legislation. Supervised institutions must send to their competent authority a description of the internal control and communications procedures they have implemented to prevent money laundering. In addition, banks must undergo

internal audits. Bureaux de change must send the Bank of Greece a monthly report on their daily purchases and sales of foreign currency and audits of such companies are also periodically carried out, albeit infrequently. However, implementation of regulatory requirements documenting the flow of large sums of cash through financial and other institutions is reportedly weak.

Under Decree 2181/93, banks in Greece must demand customer identification information when opening an account or conducting transactions that exceed 15,000 euros (approx. $19,400). If there is suspicion of illegal activities, banks may take measures to gather more information on the identification of the person involved in the transaction. If any question remains, officers must file an STR with the Bank's compliance officer, irrespective of the amount involved. Greek citizens must also provide a tax registration number if they conduct foreign currency exchanges of 1,000 euros (approx. $1300) or more. 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.

Every financial institution is required by law to appoint a compliance officer to whom all other branches or other officers must report any suspicious transactions. Reporting obligations also apply to government employees involved in auditing, including employees of the Bank of Greece, the Ministry of Economy and Finance, and the Capital Markets Commission. Reporting individuals must furnish all relevant information to the prosecuting authorities. Safe harbor provisions in Greek law protect individuals reporting violations of anti-money laundering laws and statutes.

Greece has adopted banker negligence laws under which individual bankers may be held liable if their institutions launder money. Banks and credit institutions may be subject to heavy fines if they breach their obligations to report instances of money laundering; bank officers are subject to fines and a prison term of up to two years. In September 2006, the Bank of Greece announced that for the first three-quarters of 2006, it had imposed fines in excess of ten million euros against a number of unidentified institutions for violating anti-money laundering laws and regulations. However, most of the fines reportedly require the offending institution to give the Central Bank a sum of money that the Central Bank holds in a separate, interest free account. After a designated period of time, the Central Bank returns the money to the offending institution. The Bank has imposed fines and administrative sanctions, including prohibiting the opening of new branches, in previous years.

Although authorities have recently targeted the gaming industry to restrain money launderers from using Greece's nine casinos to launder illicit funds, reportedly there is no oversight committee. Casinos are not obligated to report suspicious transactions.

Law 2331/1995 established the Competent Committee (CC), which functions as Greece's FIU. The FIU has been empowered with substantial authority. The CC is chaired by a senior retired judge and includes eleven senior representatives from the Bank of Greece, various government ministries and law enforcement agencies, the Hellenic Bankers Association, and the securities commission. The CC is responsible for receiving and processing all STRs. The STRs are hand delivered to the FIU, where, upon receipt, the committee (which is comprised of senior officials, and not full-time analysts) reviews the STRs to determine whether further investigation is necessary. If the committee requests more information from the reporting institution, the FIU will mail those questions to the institution. Once it receives a reply, the committee reviews the file again to see if the report warrants further investigation.

When the CC considers an STR to warrant further investigation, it forwards the case to the Special Control Directorate (YPEE), a multi-agency group that, in addition to initiating its own investigations, currently functions as the CC's investigative arm. When fully staffed, the Greek FIU will carry out its own investigations without resorting to help by third agencies. The YPEE, which only has investigative authority over cases which, broadly defined, involve smuggling and high-worth tax evasion, is under the direct supervision of the Ministry of Economy and Finance. The YPEE has its own in-house prosecutor in order to facilitate confidentiality and speed of action. The FIU is

responsible for preparing Money laundering cases on behalf of the Public Prosecutor's Office. The FIU is not operating at its envisaged capability because it lacks the parliamentary-approved level of full time staff, has no updated electronic database and inadequate technical capabilities for processing an ever-increasing number of STRs, which, based on unconfirmed numbers, have exceeded 1500 through late 2006.

Law 3424 passed in November 2005 upgraded the CC to an independent authority with access to public and private files, and without tax confidentiality restrictions. The law also broadens the FIU's authority with respect to the evaluation of information it receives from various organizations within Greece as well as from international organizations. However, the FIU requires a memorandum of understanding (MOU) before exchanging information with its international partners. The head of the FIU can temporarily freeze suspects' funds. The committee has the authority to impose heavy penalties on those who fail to report suspicious transactions. Reportedly, the staff limitations at the FIU have contributed to its difficulty in maintaining an effective two-way communication with Greece's broader financial community, as well as with its international counterparts.

Money laundering cases have seldom been prosecuted independently of another crime. Greek authorities do not have an effective information technology system in place to track money laundering prosecution statistics. There have been several prosecutions for money laundering in the past year. A senior judge was sentenced to 86 years in prison on charges of money laundering and receiving bribes. Additionally, the Ministry of Justice has either fired or suspended fourteen judges accused of being involved in bribery and money laundering cases. Recently, a high profile case involving over $125 million in laundered funds made headlines. It involved ten individuals and five companies spread over four countries. A court decision is still pending in the case.

If the FIU director freezes any assets, the FIU must prepare a report and forward it to an investigating magistrate and prosecutor, who conducts a further investigation and who, upon conclusion of the investigation, can issue a freezing order, pending the outcome of the criminal case. With regard to the freezing of accounts and assets, Law 3424/2005 incorporates elements of the EU Framework Decision on the freezing of funds and other financial assets, as well as the EU Council Regulation on the financing of terrorism. The GOG promulgated implementing regulations for Law 3424/2005 in June, 2006. The YPEE has established a mechanism for identifying, tracing, freezing, seizing, and forfeiting assets of narcotics-related and other serious crimes, the proceeds of which are turned over to the GOG. It is unclear what the GOG can seize once it obtains a conviction against a defendant, and whether the GOG can seize not only property as the proceeds of crime, but also property intended for use in a crime. Legitimate businesses can be seized if used to launder drug money. The GOG has not enacted laws for sharing seized narcotics-related assets with other governments.

In March 2001, the Ministry of Justice unveiled legislation on combating terrorism, organized crime, money laundering, and corruption. Parliament passed the legislation in July 2002. Under a recent counterterrorism law (Law 3251/July 2004), anyone who finances the joining or forming of a terrorist group faces imprisonment of up to ten years. If a private legal entity is implicated in terrorist financing, it faces fines of between 20,000 and 3 million euros (approximately $26,000 and $3,885,000), closure for a period of two months to two years, and ineligibility for state subsidies. Technically, it is not illegal in Greece to fund an already established terrorist group. It is only considered a terrorist financing crime if a person funds a specific attack executed by three or more people. The GOG plans to address the Financial Action Task Force's (FATF) Special Recommendation IX on cash couriers at a later date, following the issuance of a relevant EU directive.

The Bank of Greece has circulated to all financial institutions the list of individuals and entities that have been included on the UNSCR 1267 Sanctions Committee's consolidated list as being linked to Usama Bin Laden, the Al-Qaida organization, or the Taliban, as well as the EU's list of designees.

However, in most instances, there must be an active investigation before the GOG can freeze any assets. The GOG has not found any accounts belonging to anyone on the circulated lists.

The Bank of Greece maintains that alternative remittance systems do not exist in Greece and has no plans to introduce initiatives for their regulation. Illegal immigrants or individuals without valid residence permits reportedly send remittances to Albania and other destinations in the form of currency, gold and precious metals, which are often smuggled across the border in trucks and buses. The financial and economic crimes police, as well as tax authorities, closely monitor charitable and nongovernmental organizations. There is no reported evidence that such organizations are used as conduits for the financing of terrorism.

Greece is a member of the FATF, the EU, and the Council of Europe. The CC is a member of the Egmont Group. The GOG is a party to the 1988 UN Drug Convention and in December 2000 became a signatory to the UN Convention against Transnational Organized Crime, but has not yet ratified the law to enact the convention. On April 16, 2004, Greece became a party to the UN International Convention for the Suppression of the Financing of Terrorism. 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.

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.

The Government of Greece has made progress in expanding and adjusting its legislation to international standards by gradually incorporating all EU directives on money laundering and terrorist financing. However, these actions do not comprehensively address all of the FATF Forty plus Nine Recommendations. In order to meet its stated goal of effectively addressing money laundering, the Greek Government should:

- Accelerate its efforts to realize the promise of new laws and regulations aimed at upgrading its financial intelligence unit. This includes staffing it fully with experienced analysts. The FIU should also improve its information technology (IT) capabilities so that analysts can develop an comprehensive database as well as use the Egmont Group's secure communications system. These IT upgrades will have the advantage of allowing Greek authorities to implement a system to track statistics on money laundering prosecutions and convictions, as well as asset freezes and forfeitures;
- Improve its asset freezing capabilities and should develop a clear and effective system for identifying and freezing terrorist assets within its jurisdiction. Furthermore, the GOG must also make public its system for releasing any assets it may accidentally freeze in accordance with its UN obligations;
- Take steps to require suspicious transaction reporting for its casinos and for the gaming sector, and institute a supervisory body to monitor its compliance;
- Ensure uniform enforcement of its cross-border currency reporting requirements and take steps to deter the smuggling of currency and precious metals across its borders. The GOG should take steps to codify and implement legislation addressing FATF Special Recommendation IX relating to cash couriers, and not wait for an EU Directive;

- Ensure that its "Law 89" companies, and companies operating within its free trade zones, are subject to the same AML requirements and gatekeeper and due diligence provisions, including know your customer (KYC) rules and the identification of the beneficial owner, as its other sectors;
- Abolish company-issued bearer shares, so that all bearer shares are legally prohibited;
- Ratify the UN Convention against Transnational Organized Crime.

Grenada

Grenada is not an important regional financial center. Most of the money laundering found in Grenada involves smuggling and narcotics. Proceeds of narcotics trafficking may be laundered through a wide variety of businesses, as well as through the purchase of land, boats, jewelry, cars, and houses and other real estate. Grenada's offshore financial sector is also vulnerable to money laundering.

After being placed on the Financial Action Task Force's (FATF) list of noncooperative countries and territories (NCCT) in the fight against money laundering in September 2001, the Government of Grenada (GOG) implemented and strengthened its legislation and regulations necessary for adequate supervision of Grenada's offshore sector, which prompted the FATF to remove Grenada's name from the NCCT list in February 2003.

As of December 2006, Grenada had one inactive offshore bank, one trust company, one management company, and one international insurance company. Grenada is reported to have over 20 internet gaming sites. There are also nearly 6000 international business companies (IBCs). The domestic financial sector includes six commercial banks, 26 registered domestic insurance companies, two credit unions, and four or five money remitters. The GOG has repealed its economic citizenship legislation.

The Grenada International Financial Services Authority (GIFSA) monitors and regulates offshore financial services. GIFSA is governed by seven directors, appointed by the Minister of Finance, who are qualified or experienced in accounting, banking, commerce, insurance, management or law. GIFSA issues certificates of incorporation for IBCs, and makes recommendations to the Minister of Finance in regard to the revocation of offshore licenses. Bearer shares are not permitted for offshore banks. Currently Grenada's only offshore bank is inactive. However, holders of bearer shares in nonfinancial institutions or IBCs are permitted to issue bearer shares but must lodge these shares with one of the 15 or so registered agents licensed by the GIFSA. 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 directors and beneficial owners of all shares. There is an ECD 30,000 (approximately $11,500) penalty and possible revocation of the registered agent's license for failure to maintain records. The GIFSA has the ability to conduct on-site inspections; the authority to access the records and information maintained by registered agents; and the authority to obtain customer account records from an offshore institution upon request. The GIFSA is able to share this information with regulatory, supervisory and administrative agencies. The GIFSA also has access to auditors' examination reports and may also share this information with relevant authorities.

To strengthen the supervision of the nonbank financial sector, which includes the insurance sector, cooperatives, offshore financial services, and money remitters, the GOG enacted the Grenada Authority for the Regulation of Financial Institutions (GARFIN) Act in May 2006. The Act provides for the creation of a single regulatory agency responsible for regulating and supervising all nonbank financial institutions and services in Grenada. The Eastern Caribbean Central Bank has responsibility

for the supervision of domestic banks, and will continue to do so. It is anticipated that GARFIN will be operational by spring 2007.

The Money Laundering Prevention Act (MLPA) enacted in 1999 and the Proceeds of Crime Act (POCA) No. 3 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 2003, the predicate offenses for money laundering extend to all criminal conduct, which includes illicit drug trafficking, trafficking of firearms, kidnapping, extortion, corruption, terrorism and its financing, and fraud. According to the POCA 2003, a conviction on a predicate offense is not required in order to prove that certain goods are the proceeds of crime, and subsequently convict a person for laundering those proceeds. Grenada's anti-money laundering legislation applies to banks and nonbank financial institutions, as well as the offshore sector.

Established under the MLPA, the Supervisory Authority supervises the compliance of banks and nonbank financial institutions (including money remitters, stock exchange, insurance, casinos, precious gem dealers, real estate, lawyers, notaries, and accountants) with money laundering and terrorist financing laws and regulations. These institutions are required to know, record and report the identity of customers engaging in significant transactions. This applies to large currency transactions over the threshold of $3,700. Records must be maintained for seven years. In addition, a reporting entity must pay attention to 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 possibly indicative of money laundering, the reporting entity must forward a suspicious transaction report (STR) to the Supervisory Authority within 14 days.

The Supervisory Authority issued 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 them with information. Financial institutions could be fined for not granting access to Supervisory Authority personnel.

In June 2001, the GOG established a Financial Intelligence Unit (FIU), headed by a prosecutor from the Attorney General's office. The FIU's staff includes an assistant superintendent of police, four police officers, and two support personnel. In 2003, Grenada enacted the Financial Intelligence Unit Act No. 1 of 2003. Though the FIU operates within the police force, it is technically assigned to the Supervisory Authority. The FIU is charged with receiving and analyzing suspicious transaction reports (STRs) from the Supervisory Authority, and with investigating alleged money laundering offenses. From January to November 2006, the FIU received 17 STRs. An investigation of one STR resulted in an arrest, which was a joint FIU-Drug Squad operation. The operation netted a quantity of a controlled substance and $3,700. The case is currently pending in court. The FIU has the ability to directly consult bank accounts and can request any documents from institutions that it considers necessary to fulfill its functions. In addition, the FIU also has access to other government agencies' databases. The FIU has the authority to exchange information with its foreign counterparts without a memorandum of understanding (MOU).

The FIU and the Director of Public Prosecution's Office are responsible for tracing, seizing and freezing assets. The time period for restraint of property is determined by the High Court. Presently, only criminal forfeiture is allowed by law. Approximately $42,132 of criminal-related assets was seized by November 2006. The management and disposition of seized and forfeited assets are in the charge of the Minister of Finance. The POCA provides for the establishment of a confiscated assets fund; the Minister of Finance is also responsible for the management of this fund. There is no independent system for freezing terrorist assets; it falls under the general authority of the Director of

Public Prosecution. New legislation is currently under consideration, including the Civil Forfeiture Bill, Interception of Communication Act, Cash Forfeiture Act, and Confiscation of the Proceeds of Crime Bill. These bills are now being reviewed by the relevant ministries.

Grenada regulates the cross-border movement of currency. 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 between government agencies, particularly between Customs and the FIU.

The GOG criminalized terrorism financing through the Terrorism Act No. 5 2003. The legislation provides the GOG with the authority to identify, freeze, and seize assets related to terrorism. The GOG circulates to the appropriate institutions the names of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list. There has been no known identified evidence of terrorist financing in Grenada. Grenada has not taken any specific initiatives focused on alternative remittance systems or the misuse of charitable and nonprofit entities. The GOG has not identified any indigenous alternative remittance systems, but suspects there are some in operation.

A Mutual Legal Assistance Treaty and an Extradition Treaty have been in force between Grenada and the United States since 1999. Grenada also has a Tax Information Exchange Agreement (TIEA) with the United States. Grenada has cooperated extensively with U.S. law enforcement in numerous money laundering and other financial crimes investigations, contributing to successful prosecutions. Grenada also works actively with other governments to ensure asset tracing, freezing and seizures take place, if and when necessary, regardless of the status of the agreements. In 2003, the GOG passed the Exchange of Information Act No. 2 to permit the ECCB to provide information to foreign regulators on Grenadian banks, both domestic and offshore.

Grenada is a member of the Caribbean Financial Action Task Force (CFATF). The FIU became a member of the Egmont Group in June 2004. Grenada is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. The GOG is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Grenada has not yet signed the UN Convention against Corruption. On May 8, 2006, Grenada ratified the Inter-American Convention against Terrorism.

Although the Government of Grenada has strengthened the regulation and oversight of its financial sector, it must remain alert to potential abuses and must steadfastly implement the laws and regulations it has adopted. Grenada should continue to update its Anti-Money Laundering Guidelines. The GOG should also move forward in adopting civil forfeiture legislation, and establish mechanisms to identify and regulate alternative remittance systems. Law enforcement and customs authorities should initiate money laundering investigations based on regional smuggling. Grenada should also continue to enhance its information sharing, particularly with other Caribbean jurisdictions. Grenada should also become a party to the UN Convention against Corruption.

Guatemala

Guatemala is a major transit country for illegal narcotics from Colombia and precursor chemicals from Europe. Those factors, combined with historically weak law enforcement and judicial regimes, corruption and increasing organized crime activity, lead authorities to suspect that significant money laundering occurs in Guatemala. According to law enforcement sources, narcotics trafficking is the primary source of money laundered in Guatemala; however, the laundering of proceeds from other illicit sources, such as human trafficking, contraband, kidnapping, tax evasion, vehicle theft and corruption, is substantial. Officials of the Government of Guatemala (GOG) believe that couriers, offshore accounts and wire transfers are used to launder funds, which are subsequently invested in real

estate, capital goods, large commercial projects and shell companies, or are otherwise transferred through the financial system.

Guatemala is not considered a regional financial center, but it is an offshore center. Exchange controls have largely disappeared and dollar accounts are common, but some larger banks conduct significant business through their offshore subsidiaries. The Guatemalan financial services industry is comprised of 25 commercial banks, four of which exist in a state of permanent suspension with no commercial offices; ten offshore banks, all of which are affiliated, as required by law, with a domestic financial group; five licensed money exchangers; 14 money remitters, including wire remitters and remittance-targeting courier services; 18 insurance companies; 17 financial societies; 16 bonded warehouses; 308 savings and loans cooperatives; eight credit card issuers; seven leasing entities; 11 financial guarantors; and one check-clearing entity run by the Central Bank. It is also estimated that there are hundreds of unlicensed money exchangers that exist informally.

The Superintendence of Banks (SIB), which operates under the general direction of 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 money laundering concern, although proceeds from tax-related contraband are probably laundered through them.

The offshore financial sector initially offered a way to circumvent currency controls and other costly financial regulations. However, financial sector liberalization has largely removed many incentives for legitimate businesses to conduct offshore operations. All offshore institutions are subject to the same requirements as onshore institutions. In June 2002, Guatemala enacted the Banks and Financial Groups Law (No. 19-2002), which places offshore banks under the oversight of the SIB. The law requires offshore banks 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 doing business in another jurisdiction; however, banks authorized by other jurisdictions may do business in Guatemala under certain limited conditions.

In order to authorize an offshore bank, the financial group to which it belongs must first be authorized, under a 2003 resolution of the Monetary Board. By law, no offshore financial services businesses other than banks are allowed, but there is evidence that they exist in spite of that prohibition. 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, a process which resulted in the closure of two operations. No offshore trusts have been authorized, and 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 $3.5 billion in remittance flows pass through informal channels, although sector reforms are leading to increasing use of banks and other formal means of transmission. Terrorist financing legislation passed in August 2005 requires remitters to maintain name and address information on senders (principally U. S. based) on transfers equal to or over an amount to be determined by implementing regulations. Increasing financial sector competition should continue to expand services and bring more people into the formal banking sector, isolating those who abuse informal channels.

The Financial Action Task Force (FATF) placed Guatemala on the list of Non-Cooperative Countries and Territories (NCCT) in the fight against money laundering in 2001. Guatemala was removed from the NCCT list at the FATF plenary in June 2004, after authorities implemented the necessary reforms to bring Guatemala into compliance with international standards.

One of the reforms is Decree 67-2001, or the "Law Against Money and Asset Laundering." 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 will be expelled from Guatemala. Conspiracy and attempt to commit money laundering are also penalized. The law holds institutions and businesses responsible for failure to prevent money laundering or allowing money laundering to occur, regardless of the responsibility of owners, directors or other employees, and they may face cancellation of their banking licenses and/or criminal charges. The law also applies to the offshore entities that operate in Guatemala but are registered under the laws of another jurisdiction.

Decree 67-2001 also obligates individuals and legal entities to report to the competent authorities the cross-border movement of currency in excess of approximately $10,000. At Guatemala City airport, a new special unit was formed in 2003 to enforce the use of customs declarations upon entry to and exit from Guatemala. Money seized at the airports—approximately $167,400 in 2006—suggests that proceeds from illicit activity are regularly hand carried over Guatemalan borders. However, apart from a cursory check of a self-reporting customs form, there is little monitoring of compliance at the airport. Compliance is not regularly monitored at land borders.

In addition, the Guatemalan Monetary Board issued Resolution JM-191, approving the "Regulation to Prevent and Detect the Laundering of Assets" (RPDLA) submitted by the SIB. The RPDLA requires all financial institutions under the oversight and inspection of the SIB to establish anti-money laundering measures, and introduces 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.

Covered institutions are prohibited from maintaining anonymous accounts or accounts that appear under fictitious or inexact names. Nonbank financial institutions, however, may issue bearer shares, and there is limited banking secrecy. Obligated entities are required to keep a registry of their customers as well as of the transactions undertaken by them, 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 Guatemala's FIU, the IVE. Under the law, obligated entities must maintain records of these registries and transactions for five years. Financial institutions are also required to report all suspicious transactions to the IVE.

Decree 67-2001 establishes the IVE within the Superintendence of Banks in order to supervise covered financial institutions and ensure their compliance with the law. The IVE began operations in 2002 and has a staff of 26. 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 on the covered entities' management, compliance officers, anti-money laundering training programs, "know-your-client" policies, and auditing programs. The IVE has imposed over $100,000 in civil penalties to date for institutional failure to comply with anti-money laundering regulation.

Since its inception, the IVE has received approximately 1,600 suspicious transaction reports (STRs) from the 400 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. Bank secrecy can be lifted for the investigation of money laundering crimes. 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. The IVE also assists the Public Ministry by providing information upon request for other cases the prosecutors are investigating.

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, Prosecutor's Office, Government Ministry, National Police and Drug Police. Together they work on investigating financial crimes, building evidence and bringing the cases to prosecution. They are currently working on four cases of suspected money laundering.

Other government agencies have become involved in combating money laundering. In addition to the SIB, the SAT has been working to improve its processes and personnel to better collect taxes and combat tax evasion. This indirectly assists anti-money laundering efforts by making it easier to detect suspicious activity through nonpayment of tax.

Thirty-nine cases have been referred by the IVE to the AML Unit, four of which stem from public corruption. In several cases, assets have been frozen. Thirteen money laundering prosecutions have been concluded, twelve of which resulted in convictions. Eleven of those cases have been sentenced, with the remaining two cases awaiting the completion of appeals. Additional cases have been developed from cooperation between the Public Ministry and the IVE. The Public Ministry's AML Unit had initiated 46 cases as of January 2006. In addition, four cases have been transferred to other offices for investigation and prosecution (such as the anticorruption unit) due to the nature of their particular predicate offenses. The other 46 cases are either still under investigation or in initial trial stages. Several high profile cases of laundering proceeds from major corruption scandals involving officials of the previous government are currently under investigation and have resulted in arrests and substantial seizures of funds and assets. These seizures have been supported by the cooperating financial institutions along with the vast majority of public and political interests.

In 2006, Guatemala passed an organized crime control law. This new legislation permits the use of undercover operations, controlled deliveries and wire taps to investigate many forms of organized crime activity, including money laundering crimes.

Under current legislation, any assets linked to money laundering can be seized. The IVE, the National Civil Police, and the Public Ministry have the authority to trace assets; the Public Ministry can seize assets temporarily or in urgent cases, and the Courts of Justice have the authority to permanently seize assets. In 2003, the Guatemalan Congress approved reforms to enable seized money to be shared among several GOG agencies, including police and the IVE. Nevertheless, the Constitutional Court ruled that forfeited currency remains under the jurisdiction of the Supreme Court of Justice.

An additional problem is that the courts do not allow seized currency to benefit 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 2005, Guatemalan authorities seized more than U.S. $6.5 million in bulk currency, significantly less that the $20 million seized in 2003 (although one case alone in 2003 accounted for more than $14 million). 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 June 2005, the Guatemalan Congress passed legislation criminalizing terrorist financing. Implementing regulations were submitted to the Monetary Board in December 2005. According to the GOG, Article 391 of the penal code already sanctioned all preparatory acts leading up to a crime, and financing would likely be considered a preparatory act. Technically, both judges and prosecutors could have issued a freeze order on terrorist assets, but no test case ever validated these procedures. The new counterterrorism financing legislation removed potential uncertainty regarding the legality of freezing

assets when no predicate offense had been legally established but the assets have been determined destined to terrorists or to support terrorist acts. The GOG has been very cooperative in looking for terrorist financing funds. The new legislation brings Guatemala into greater compliance with FATF Special Recommendations on Terrorist Financing and the United Nations Security Council Resolution 1373 Against Terrorism.

Guatemala is a party to the UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. On March 1, 2006, the GOG ratified the Inter-American Convention against Terrorism, and on November 3, 2006, the GOG ratified the UN Convention against Corruption. Guatemala is also a party to the Central American Convention for the Prevention of Money Laundering and Related Crimes. 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 (CFATF). In 2003, the IVE became a member of the Egmont Group.

Corruption and organized crime remain strong forces in Guatemala and may prove to be the biggest hurdles facing the Government of Guatemala in the long term. Guatemala has made efforts to comply with international standards and improve its anti-money laundering regime; however, Guatemala should take steps to immobilize bearer shares, and to identify and regulate offshore financial services and gaming establishments. The GOG should also continue efforts to improve enforcement and implementation of needed reforms. Cooperation between the IVE and the Public Ministry has improved since the new administration took office in January 2004, and several investigations have led to prosecutions. However, Guatemala should continue to focus its efforts on boosting its ability to successfully investigate and successfully prosecute money laundering cases, and distributing seized assets to law enforcement agencies to assist in the fight against money laundering and other financial crime.

Guernsey

The Bailiwick of Guernsey (the Bailiwick) covers a number of the Channel Islands (Guernsey, Alderney, Sark, and Herm in order of size and population). The Islands are dependents of the British Crown and the United Kingdom (UK) is responsible for their 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 law for all of the islands in the Bailiwick. The Bailiwick alone has authority to legislate domestic taxation. The Bailiwick is a sophisticated financial center and, as such, it continues to be vulnerable to money laundering at the layering and integration stages.

There are approximately 17,800 companies registered in the Bailiwick. Nonresidents own approximately half of the companies, and they have an exempt tax status. These companies do not fall within the standard definition of an international business company (IBC). Local residents own the remainder of the companies, including trading and private investment companies. Exempt companies are not prohibited from conducting business in the Bailiwick, but must pay taxes on profits of any business conducted on the islands. Companies can be incorporated in Guernsey and Alderney, but not in Sark, which has no company legislation. Companies in Guernsey may not be formed or acquired without disclosure of beneficial ownership to the Guernsey Financial Services Commission (the Commission).

Guernsey has 51 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 626 international insurance companies and 684 collective investment funds. There are also 18 bureaux de change, which file accounts with the tax authorities. Ten of the bureaux de change are part of a

licensed bank, and it is the bank that publishes and files those accounts. Bureaux de change and other money service providers are required to register information with the Commission.

Guernsey has put in place a comprehensive legal framework to counter money laundering and the financing of terrorism. The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law 1999, as amended, is supplemented by the Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) Regulations, 2002. The legislation criminalizes money laundering for all crimes except drug-trafficking, which is covered by the Drug Trafficking (Bailiwick of Guernsey) Law, 2000. The Proceeds of Crime Law and the Regulations are supplemented by Guidance Notes on the Prevention of Money Laundering and Countering the Financing of Terrorism, issued by the Commission. There is no exemption for fiscal offenses. The 1999 law creates a system of suspicious transaction reporting (including tax evasion) to the Guernsey Financial Intelligence Service (FIS). The Bailiwick narcotics trafficking, anti-money laundering, and terrorism laws designate the same foreign countries as the UK to enforce foreign restraint and confiscation orders.

The Drug Trafficking (Bailiwick of Guernsey) Law 2000 consolidates and extends money laundering legislation related to narcotics trafficking. It introduces the offense of failing to disclose the knowledge or suspicion of drug money laundering. The duty to disclose extends beyond financial institutions to cover others as well, for example, bureaux de change and check cashers.

In addition, the Bailiwick authorities enacted the Prevention of Corruption (Bailiwick of Guernsey) Law of 2003. They have also resolved to merge existing drug trafficking, money laundering and other crimes into one statute, and to introduce a civil forfeiture law.

On April 1, 2001, the Regulation of Fiduciaries, Administration Businesses, and Company Directors, etc. (Bailiwick of Guernsey) Law of 2000 ("the Fiduciary Law") came into effect. The Fiduciary Law was enacted to license, regulate and supervise company and trust service providers. Under Section 35 of the Fiduciary Law, the Commission creates Codes of Practice for corporate service providers, trust service providers and company directors. Under the law, the Commission must license all fiduciaries, corporate service providers and persons acting as company directors on behalf of any business. In order to be licensed, these agencies must pass strict tests. These include "know your customer" requirements and the identification of clients. These organizations are subject to regular inspection, and failure to comply could result in the fiduciary being prosecuted and/or its license being revoked. The Bailiwick is fully compliant with the Offshore Group of Banking Supervisors Statement of Best Practice for Company and Trust Service Providers.

Since 1988, the Commission has regulated the Bailiwick's financial services businesses. The Commission regulates 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 "know your customer" inquiry and verification details are provided. The AML/CFT Regulations contain penalties to be applied when financial services businesses do not follow the requirements of the Regulations. Company incorporation is by act of the Royal Court, which maintains the registry. All applications to form a Bailiwick company have to be made to the Commission, which then evaluates each application. The Court will not permit incorporation unless the Commission and the Attorney General or Solicitor General has given prior approval. The Commission conducts regular on-site inspections and analyzes the accounts of all regulated institutions.

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.

Under the retention tax option, each financial services provider will automatically deduct tax from interest and other savings income paid to EU resident individuals. The tax will then be submitted to local and Member States tax authorities annually. The tax authorities receive a bulk payment but do not receive personal details of individual customers. If individuals elect the exchange of information option, then no tax is deducted from their interest payments but details of the customer's identity, residence, paying agent, level and time period of savings income received by the financial services provider will be reported to local tax authorities where the account is held and then forwarded to the country where the customer resides.

The Guernsey authorities have established a forum, the Crown Dependencies Anti-Money Laundering Group, where the Attorneys General from the Crown Dependencies, Directors General and other representatives of the regulatory bodies, and representatives of police, Customs, and the Financial Intelligence Service (FIS) meet to coordinate the anti-money laundering and counterterrorism policies and strategy in the Dependencies.

The FIS operates as the Bailiwick's financial intelligence unit (FIU). The FIS began operations in April 2001, and is currently staffed by Police and Customs/Excise Officers. The FIS is directed by the Service Authority, which is a small committee of senior Police and Customs Officers who co-ordinate with the Bailiwick's financial crime strategy and report to the Chief Officers of Police and Customs/Excise. The FIS is mandated to place specific focus and priority on money laundering and terrorism financing issues. Suspicious Transaction Reports (STRs) are filed with the FIS, which serves as the central point within the Bailiwick for the receipt, collation, analysis, and dissemination of all financial crime intelligence. In 2005, the FIS received 650 STRs. The FIS received 757 STRs in 2004 and 705 STRs in 2003.

In November 2002, the International Monetary Fund (IMF) undertook an assessment of Guernsey's compliance with internationally accepted standards and measures of good practice relative to its regulatory and supervisory arrangements for the financial sector. The IMF report states that Guernsey has a comprehensive system of financial sector regulation with a high level of compliance with international standards. As for AML/CFT, the IMF report highlights that Guernsey has a developed legal and institutional framework for AML/CFT and a high level of compliance with the FATF Recommendations.

There has been counterterrorism legislation covering the Bailiwick since 1974. The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002, replicates equivalent UK legislation.

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. Guernsey cooperates with international law enforcement on money laundering cases. 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. The Commission also cooperates with regulatory/supervisory and law enforcement bodies.

On September 19, 2002, the United States and Guernsey signed a Tax Information Exchange Agreement, which is not yet in force. 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. Currently, similar agreements are being negotiated with other countries, among them members of the European Union.

After its extension to the Bailiwick, Guernsey enacted the necessary legislation to implement the Council of Europe Convention on Mutual Assistance in Criminal Matters, the Council of Europe

Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, and the 1988 UN Drug Convention. 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. The Bailiwick has requested that the UK Government seek the extension to the Bailiwick of the UN International Convention for the Suppression of the Financing of Terrorism.

The Attorney General's Office is represented in the European Judicial Network and has participated in the European Union's PHARE anti-money laundering developmental assistance project. The Commission cooperates with regulatory/supervisory and law enforcement bodies. It is a member of the International Association of Insurance Supervisors, the Offshore Group of Insurance Supervisors, the Association of International Fraud Agencies, the International Organization of Securities Commissions, the Enlarged Contact Group for the Supervision of Collective Investment Funds, and the Offshore Group of Banking Supervisors. The FIS is a member of the Egmont Group.

Guernsey has put in place a comprehensive anti-money laundering regime, and has demonstrated its ongoing commitment to fighting financial crime. Bailiwick officials should continue both to carefully monitor Guernsey's anti-money laundering program to assure its effectiveness, and to cooperate with international anti-money laundering authorities.

Guyana

Guyana is neither an important regional nor an offshore financial center, nor does it have any free trade zones. However, the scale of money laundering is thought to be large relative to the size of the economy, with some experts estimating that the informal economy is 40 to 60 percent of the size of the formal sector. Money laundering has been linked to trafficking in drugs, firearms and persons, as well as to corruption and fraud. Drug trafficking and money laundering appear to be benefiting the Guyanese economy, particularly the construction sector. Investigating and prosecuting money laundering cases is not a priority for law enforcement. The Government of Guyana (GOG) made no arrests or prosecutions for money laundering in 2006 due to a lack of adequate legislation and resources.

The Money Laundering Prevention Act of 2000 criminalizes money laundering related to narcotics trafficking, illicit trafficking of firearms, extortion, corruption, bribery, fraud, counterfeiting and forgery. The Act does not specifically cover the financing of terrorism or all serious crimes in its list of offenses. Licensed financial institutions—including banks, securities brokers, exchange houses, credit unions, building societies and trusts—are required to report suspicious transactions to Guyana's financial intelligence unit (FIU), although they are left to determine thresholds individually according to banking best practices. Financial institutions must keep records of suspicious transaction reports (STRs) for six years. The law also requires that the cross-border transportation of currency exceeding $10,000 be reported. The legislation includes provisions regarding confidentiality in the reporting process, good faith reporting, penalties for destroying records related to an investigation or disclosing investigations, and international cooperation. The Money Laundering Prevention Act 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 crime.

The GOG's anti-money laundering regime is ineffective, and the implementing regulations of the Money Laundering Prevention Act are inadequate. Guyana's central bank, the Bank of Guyana, lacks the capacity to fully execute its mandate to supervise financial institutions for compliance with anti-money laundering provisions. There have been no money laundering prosecutions to date, and it is unclear if a conviction for the predicate offense is necessary to obtain a money laundering conviction. The financial intelligence unit, established within the Ministry of Finance in 2003, is currently a one-person organization and is dependent upon the Ministry for its budget and office space. Although the

FIU may request additional information from obligated entities, its analytical capabilities are severely limited by its inability to access to law enforcement data and its lack of authority to exchange information with foreign FIUs. The GOG does not release statistics on the number of suspicious transaction reports received by the FIU, although the requirement to make these statistics available to relevant authorities is mandated by the Financial Action Task Force (FATF).

In order to improve the GOG's anti-money laundering regime, the FIU has prepared drafts of legislation criminalizing the financing of terrorism and expanding the scope of the money laundering offense. The new legislation is also expected to provide for oversight of export industries, the insurance industry, real estate and alternative remittance systems. The draft money laundering act failed to make the legislative agenda before the dissolution of Parliament in May 2006.

In January 2007, the National Assembly passed the Gambling Prevention (Amendment) Bill, which legalizes casino gambling. The bill establishes a Gaming Authority authorized to issue casino licenses to new luxury hotel or resort complexes with a minimum of 150 rooms. Vocal opposition to the bill from religious groups, opposition parties, and the public included concerns that casino gambling would provide a front for money launderers.

The Money Laundering Prevention Act provides for seizure of assets derived as proceeds of crime, including money, investments, and real and personal property. However, guidelines for implementing seizures and forfeitures have not been finalized. Forfeiture and seizure mechanisms are conviction-based, and may be carried out by the Office of the Director of Public Prosecutions if a court order is obtained.

The Ministry of Foreign Affairs and the Bank of Guyana continue to assist U.S. efforts to combat terrorist financing by working towards 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 underwent its second CFATF mutual evaluation in 2004, and the results of the evaluation were presented at the CFATF plenary in October 2006. The mutual evaluation team found the GOG to be noncompliant or materially noncompliant with approximately half of the FATF Recommendations.

Guyana is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. Guyana has not signed the UN International Convention for the Suppression of the Financing of Terrorism or the UN Convention against Corruption. The GOG has signed, but not yet ratified, the Inter-American Convention against Terrorism. Guyana's FIU is one of the few in the region that is not a member of the Egmont Group.

The Government of Guyana should introduce the draft legislation on money laundering to Parliament early in the legislative session. The GOG should provide greater autonomy for the FIU by making it an independent unit with its own budget and office space, 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 and other international standards. Guyana should also provide appropriate resources and awareness training to its regulatory, law enforcement and prosecutorial personnel, and establish procedures for asset seizure and forfeiture. Now that Guyana has legalized casino gambling, the GOG should ensure that the necessary anti-money laundering regulations are extended to the gaming sector. Guyana should criminalize terrorist financing and adopt measures that would allow it to block terrorist assets. In addition, Guyana should seize opportunities to sensitize the public to the harmful impact of money laundering on legitimate businesses and the national economy. The GOG should become a party to the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Corruption.

Haiti

Haiti is not a major financial center. Given Haiti's dire economic condition and unstable political situation, it is doubtful that it will become a major player in the region's formal financial sector in the near future. Haiti is a major drug-transit country, and money laundering activity is linked to the drug trade. Money laundering and other financial crimes occur in the banking system and in casinos, foreign currency transactions 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. Flights to Panama City, Panama, remain the main identifiable mode of transportation for money couriers. Usually travelers, predominantly Haitian citizens, hide large sums, ranging from $30,000 to $100,000 on their persons. Haitian narcotics officers interdicting these outbound funds often collect a six to 12 percent fee and allow the couriers to continue without arrest. During interviews, couriers usually declare that they intend to use the large amounts of U.S. currency to purchase clothing and other items to be sold upon their return to Haiti, a common practice in the informal economic sector. Further complicating the picture is the cash that is routinely transported to Haiti from Haitians and their relatives in the United States in the form of remittances, representing an estimated 30 percent of Haiti's gross domestic product.

In March 2004, an interim government was established in Haiti following former President Jean Bertrand Aristide's resignation and departure. The Interim Government of Haiti (IGOH) took initiatives to establish improvements in economic and monetary policies, as well as working to improve governance and transparency. In response to the corruption that continues to plague Haiti, the IGOH created an Anti-Corruption Unit and a commission to examine transactions conducted by the government from 2001 through February 2004. The commission published its report in July 2005. In early 2006 Presidential elections took place. Neither the IGOH nor the new government have prosecuted any cases based on the information provided in the report.

Despite political instability, Haiti has taken steps to address its money laundering and financial crimes problems. Since 2001, Haiti has used the Law on Money Laundering from Illicit Drug Trafficking and other Crimes and Punishable Offenses (AML Law) as its primary anti-money laundering legislation. All financial institutions and natural persons are subject to the money laundering controls of the AML Law. The AML Law criminalizes money laundering and applies to a wide range of financial institutions, including banks, money remitters, exchange houses, casinos, and real estate agents. Insurance companies are not covered; however, they are only nominally represented in Haiti. The AML Law requires financial institutions to establish money laundering prevention programs and to verify the identity of customers who open accounts or conduct transactions that exceed 200,000 gourdes (approximately $5,420). It also requires exchange brokers and money remitters to obtain declarations identifying the source of funds exceeding 200,000 gourdes or its equivalent in foreign currency. The nonfinancial sector, however, remains largely unregulated.

In 2002, Haiti formed a National Committee to Fight Money Laundering, the Comité National de Lutte Contre le Blanchiment des Avoirs (CNLBA). 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. Created in 2003, the Unite Centrale de Renseignements Financiers (UCREF) is the financial intelligence unit (FIU) of Haiti. The UCREF is responsible for receiving and analyzing reports submitted in accordance with the law. The UCREF has approximately 42 employees, including 25 investigators. Institutions are required to report to the UCREF any transaction involving funds that appear to be derived from a crime, as well as those exceeding 200,000 gourdes. Failure to report such transactions is punishable by more than three years' imprisonment and a fine of 20 million gourdes (approximately $542,000). Banks are required to maintain records for at least five years and are required 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.

The AML Law has provisions for the forfeiture and seizure of assets; however the government cannot declare the asset or business forfeited until there is a conviction. The inability to seize or freeze assets early in the judicial process reduces the government's authority and resources to pursue cases. The IGOH was supportive of a stronger, more proactive asset seizure law, yet its temporary governmental mandate did not allow for the passage of new laws. The IGOH set-up a Financial Crimes Task Force under the auspices of the Central Bank and the Ministries of Justice and Finance, charged with identifying and investigating major financial crimes and coordinating with the UCREF in recommending prosecutions. The recently elected Government of Haiti has not recognized the Task Force and the Task Force has become dormant.

In 2006, UCREF confiscated $801,000 and froze 157 million gourdes (approximately $4.3 million), in addition to $1.4 million related to money laundering offenses. It is unknown how many current investigations are active at this time. The director of UCREF was jailed for a short period of time by a magistrate on unknown charges. At the time of his incarceration over $1.4 million was unfrozen and released to the persons who claimed ownership.

In 2006 the UCREF assisted the U.S. in at least three major investigations. The UCREF also assisted the IGOH in filing the first-ever civil lawsuit in a U.S. court for reparation of Haitian government funds diverted through U.S. banks and businesses. However, the law suit was dropped shortly after the new government took office. Though the recent achievements of the UCREF are a marked improvement, it is still not fully functional or funded, and many of the UCREF's employees still lack experience and the ability to independently investigate cases, which translates into slow progress in moving cases into the judicial system.

Haiti still has not passed legislation specifically criminalizing the financing of terrorists and terrorism, nor has it signed the UN International Convention for the Suppression of the Financing of Terrorism. Reportedly, Haiti does circulate the UN 1267 list. The AML Law provides for investigation and prosecution in all cases of illegally derived money. Under this law, terrorist finance assets may be frozen and seized. Currently, there is no indication of the financing of terrorism in Haiti.

Haiti is a party to the 1988 UN Drug Convention, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption and the Inter-American Convention against Terrorism. Haiti is a member of the OAS/CICAD Experts Group to Control Money Laundering and the Caribbean Financial Action Task Force. The UCREF is not a member of the Egmont Group of financial intelligence units; however, it has three memoranda of understanding with the FIUs of the Dominican Republic, Panama and Honduras.

While improvements were made to Haiti's anti-money laundering regime under the IGOH, the new administration should implement and enforce the AML Law. The Government of Haiti should confront the rampant corruption present in almost all public institutions. The GOH should recognize the Financial Crimes Task Force and should strengthen the organizational structures and personal skills of employees both in the UCREF and the Financial Crimes Task Force. Steps should be taken so

that the UCREF fully meets international standards and is eligible for membership in the Egmont Group. The GOH should enact legislation to criminalize the financing of terrorism and become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

Honduras

Honduras is not an important regional or offshore financial center and is not considered to have a significant black market for smuggled goods, although there have been recent high-profile smuggling cases involving gasoline and other consumer goods. Money laundering, however, does take place, primarily through the banking sector but also through currency exchange houses and front companies. The vulnerabilities of Honduras to money laundering stem primarily from significant trafficking of narcotics, particularly cocaine, throughout the region. An estimated $2 billion in remittances and smuggling of contraband may also generate funds that are laundered through the banking system. Money laundering in Honduras derives both from domestic and foreign criminal activity, and the proceeds are controlled by local drug trafficking organizations and organized crime syndicates. Honduras is not experiencing an increase in financial crimes such as bank fraud. It is not a matter of government policy to encourage, facilitate or engage in laundering the proceeds from illegal drug transactions, terrorist financing or other serious crimes. However, corruption remains a serious problem, particularly within the judiciary and law enforcement sectors.

There is no indication Honduran free trade zone companies are being used in trade-based money laundering schemes or by financiers of terrorism. Under Honduran legislation, companies may register for "free trade zone" status, and benefit from the associated tax benefits, regardless of their location in the country. Companies that wish to receive free trade zone status must register within the Office of Productive Sectors within the Ministry of Industry and Commerce. The majority of companies with free trade zone status operate mostly in the textile and apparel industry.

Money laundering has been a criminal offense in Honduras since 1998, when the passage of Law No. 27-98 criminalized the laundering of narcotics-related proceeds and introduced various record keeping and reporting requirements for financial institutions. However, weaknesses in the law, including a narrow definition of money laundering, made it virtually impossible to successfully prosecute the crime.

In 2002, Honduras passed Decree No. 45-2002, which strengthened its legal framework and available investigative and prosecutorial tools to fight money laundering. Under the new legislation, the definition of money laundering was expanded to include the 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 a prison sentence of 15-20 years. The law also requires all persons entering or leaving Honduras to declare-and, if asked, present-cash and convertible securities (títulos valores de convertibilidad inmediata) that they are carrying if the amount exceeds $10,000 or its equivalent.

Decree No. 45-2002 created the financial intelligence unit (FIU), the Unidad de Información Financiera (UIF), within the National Banking and Securities Commission. Banks and other financial institutions are required to report to the UIF currency transactions over $10,000 in dollar denominated accounts or the equivalent in local currency accounts, as well as all suspicious transactions. The law requires the UIF and reporting institutions to 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 a client's deposits, and to keep adequate records of the information. The law also includes banker negligence provisions that make individual bankers subject to two- to five-year prison terms if, by carelessness, negligence, inexperience or non-observance 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 National Banking and Securities Commission, including state and private banks, savings and loan associations, bonded warehouses, stock markets, currency exchange houses, securities dealers, insurance companies, credit associations, and casinos.

Decree No. 45-2002 requires that a public prosecutor be assigned to the UIF. In practice, two prosecutors are assigned to the UIF, each on a part-time basis, with responsibility for specific cases divided among them depending upon their expertise. The prosecutors, under urgent conditions and with special authorization, may subpoena data and information directly from financial institutions. Public prosecutors and police investigators are permitted to use electronic surveillance techniques to investigate money laundering.

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 have alleged that their personal security is put at risk if the information they report leads to the prosecution of money launderers. This has not been an issue throughout 2006, however, as only cases originating from the police and prosecutors have been presented in court.

There had been some ambiguity in Honduran law concerning the responsibility of banks to report information to the supervisory authorities, and the duty of these institutions to keep customer information confidential. A new law passed in September 2004, the Financial Systems Law (Decree No. 129-2004), clarifies this ambiguity, explicitly stating that the provision of information requested by regulatory, judicial, or other legal authorities shall not be regarded as an improper divulgence of confidential information.

In December 2004, Decree No. 24-2004 created the Interagency Commission for the Prevention of Money Laundering and Financing of Terrorism (CIPLAFT). The group was tasked as the coordinating entity responsible for ensuring that all anti-money laundering and anti-financing of terrorism systems operate efficiently and consistently with all relevant laws, regulations, resolutions, and directives. However, the size of the group and overly political environment stifled effective discussions and marginalized any positive developments that came out of the meetings. In early 2006, the new head of the banking commission effectively terminated the CIPLAFT.

At roughly the same time as the termination of the CIPLAFT, a new agreement among the Public Ministry, the banking commission, and the UIF was drafted with the intent to more effectively prioritize money laundering cases and determine which cases to pursue. Previously, an average of 20 nonpriority cases were sent to prosecutors for review each month. This has been streamlined to a more manageable five cases, each of which has been determined to be promising for potential prosecution, and many older cases have been officially closed. The result is fewer active cases, allowing the overloaded prosecutors and under-funded police units to focus on the strongest and most important cases.

Prior to 2004, there had been no successful prosecutions of money laundering crimes in Honduras. In 2004, however, Honduran authorities arrested 16 persons for money laundering crimes, issued six additional outstanding arrest warrants, and secured five convictions. Through November of 2006, another six convictions have been obtained.

The Honduran Congress first enacted an asset seizure law in 1993. Decree No. 45-2002 strengthens the asset seizure provisions of the law, and established an Office of Seized Assets (OABI) under the Public Ministry. Decree 45-2002 authorizes the OABI to guard and administer all goods, products or instruments of a crime, and states that money seized or money raised from the auctioning of seized goods should be transferred to the public entities that participated in the investigation and prosecution of the crime. Under the Criminal Procedure Code, when goods or money 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.

Decree No. 45-2002 is not entirely clear on the issue of whether a legitimate business can be seized if used to launder money derived from criminal activities. The chief prosecutor for organized crime maintains that the authorities do have this power, because once a "legitimate" business is used to launder criminal assets, it ceases to be "legitimate" and is subject to seizure proceedings. However, this authority is not explicitly granted in the law, and there has been no test case to date which would set an interpretation. There are currently no new laws being considered regarding seizure or forfeiture of assets of criminal activity.

As of December 2006, the total value of assets seized since the 2002 law came into effect is estimated at $5.7 million, including $4.6 million in tangible assets such as cars, houses and boats. To date in 2006, two new cases have added approximately $20,000 to the total assets seized. Most of these seized assets are alleged to have derived from crimes related to drug trafficking; none is suspected of being connected to terrorist activity. The law allows for both civil and criminal forfeiture, and there are no significant legal loopholes that allow criminals to shield their assets.

In addition to undergoing the financial audit verifying the bank accounts, OABI has moved to distribute funds to various law enforcement units and nongovernmental organizations (NGOs). The funds, which constituted the first systematic distribution under the new guidelines, went to the Supreme Court, federal prosecutors, OABI, and two civil society groups. 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 or high protection and maintenance fees. With new management and guidelines in place, OABI is set to expand its role significantly when a witness protection law passes that will allow the unit to hold all seized assets, not just assets seized under the money laundering law.

The GOH has been supportive of counterterrorism efforts. Decree No. 45-2002 states that an asset transfer related to terrorism is a crime; however, terrorist financing has not been identified as a crime itself. This law does not explicitly grant the GOH the authority to freeze or seize terrorist assets; however, under separate authority, the National Banking and Insurance Commission has issued freeze orders promptly for the organizations and individuals named by the United Nations 1267 Sanctions Committee and those organizations and individuals on the list of Specially Designated Global Terrorists designated by the United States pursuant to Executive Order 13224. The Ministry of Foreign Affairs is responsible for instructing the Commission to issue freeze orders. The Commission directs Honduran financial institutions to search for, hold and report on terrorist-linked accounts and transactions, which, if found, would be frozen. The Commission has reported that, to date, no accounts linked to the entities or individuals on the lists have been found in the Honduran financial system.

While Honduras is a major recipient of flows of remittances (estimated at $2 billion in 2006), there has been no evidence to date linking these remittances to the financing of terrorism. Remittances primarily flow from Hondurans living in the United States to their relatives in Honduras. Most remittances are sent through wire transfer or bank services, with some cash probably being transported physically from the United States to Honduras. There is no significant indigenous alternative remittance system operating in Honduras, nor is there any evidence that charitable or nonprofit entities in Honduras have been used as conduits for the financing of terrorism.

Honduras cooperates with U.S. investigations and requests for information pursuant to the 1988 United Nations Drug Convention. No specific written agreement exists between the United States 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 and the Dominican Republic.

Honduras is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Corruption, and the Inter-American Convention against Terrorism. Honduras strives to comply with the Basel Committee's "Core Principles for Effective Banking Supervision," and the new Financial System Law, Decree No. 129-2004, is designed to improve compliance with these international standards. 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). In 2005, the UIF became a member of the Egmont Group.

Four years after passing a new law against money laundering, the Government of Honduras (GOH) continued to make considerable progress in implementing the law, establishing and training the entities responsible for the investigation of financial crimes, and improving cooperation among these entities. In 2006, the Government of Honduras continues its positive steps to implement Decree No. 45-2002. The number of good cases identified for investigation has helped focus the poorly funded prosecutors and police force, while the number of cases closed continues to climb. The asset seizure organization, OABI, continues to improve, and seized assets could soon become a significant funding source for the Public Ministry and police forces. The GOH should continue to support the developing law enforcement and regulatory entities responsible for combating money laundering and other financial crimes, and ensure that resources are available to strengthen its anti-money laundering regime. Sustained progress will depend upon increased commitment from the government to aggressively prosecute financial crimes. Honduras should draft and pass legislation specifically criminalizing the financing of terrorism to comport with international standards.

Hong Kong

Hong Kong is a major international financial center. Its low taxes and simplified tax system, sophisticated banking system, the availability of secretarial services and 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 primary sources of laundered funds are tax evasion, fraud, illegal gambling and bookmaking, and intellectual property rights violations. Laundering channels include Hong Kong's banking system, and its legitimate and underground remittance and money transfer networks. The proceeds from narcotics trafficking are believed to be only a small percentage of illicit proceeds laundered. However, over the past two years, reportedly legitimate Hong Kong business entities and financial institutions have been playing an increasingly important role in the Black Market Peso Exchange (BMPE). The BMPE in Hong Kong is perpetuated by local Hong Kong business entities that either knowingly or unknowingly enter into business agreements with individuals directly associated with the BMPE process. The BMPE is a trade-based money laundering scheme used by Colombian drug cartels to launder illicit drug profits. Hong Kong is substantially in compliance with the Financial Action Task Force's (FATF) Forty Recommendations on Money Laundering, and has pledged to adhere to the revised FATF Forty Recommendations. It is a regional leader in anti-money laundering efforts. Hong Kong has been a member of the FATF since 1990.

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 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 $641,000).

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). 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 or 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.

Financial regulatory authorities 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 Hong Kong Monetary Authority is responsible for supervising and examining compliance of financial institutions that are authorized under Hong Kong's Banking Ordinance. The Hong Kong Securities and Futures Commission (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 Office of the Commissioner of Insurance (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 money changers must register their businesses with the police and keep customer identification and transaction records for cash transactions equal to or over HK$20,000 (approximately $2,564), and must retain these records for at least six years. Under a directive from Hong Kong's Monetary Authority, Hong Kong would reduce this threshold amount to HK$8000 (approximately $1000) effective January 1, 2007.

Hong Kong 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. 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 the recommended "declaration system." Law enforcement agents in Hong Kong are already empowered to seize criminal proceeds at any place, including at the border.

There is no distinction made in Hong Kong between onshore and offshore entities, including banks, and no differential treatment is provided for nonresidents, including on taxes, exchange controls, or disclosure of information regarding the beneficial owner of accounts or other legal entities. Hong Kong's financial regulatory regimes are applicable to residents and nonresidents alike. 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. Hong Kong registered 7,279 new international business companies (IBCs) in 2005. Many of the more than 500,000 IBCs created in Hong Kong are owned by other IBCs registered in the British Virgin Islands. Many of the IBCs are established with nominee directors. The concealment of the ownership of accounts and assets is ideal for the laundering of funds. Additionally, some banks permit the shell companies to open bank accounts based only on the vouching of the company formation agent. In such cases, the HKMA's anti-money laundering guidelines require banks to verify the identity of the

owners of the company, including beneficial owners. The bank should also assess whether the intermediary is "fit and proper." However, solicitors and accountants have filed a low number of suspicious transaction reports in recent years, and consequently have become a focus of attention to improve reporting through regulatory requirements and oversight.

The open nature of Hong Kong's financial system has long made it the primary conduit for funds being 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- (renminbi or RMB) based deposit, exchange, and remittance services. Later in the 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 signed up to 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 to clients. The new provisions raised daily limits and expanded services. Making loans in Hong Kong in RMB, however, is still not permitted for any bank. 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.

Under the Drug Trafficking (Recovery of Proceeds) Ordinance (DTRoP) and the Organized and Serious Crimes Ordinance (OSCO), a court may issue a restraining order against a defendant's property at or near the time criminal proceedings are instituted. Both ordinances were strengthened in January 2003, through a legislative amendment lowering the evidentiary threshold for initiating confiscation and restraint orders against persons or properties suspected of drug trafficking. 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 the defendant or one of the defendants. 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.

Hong Kong Customs and Hong Kong Police are responsible for conducting financial investigations. 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.

As of October 31, 2006, the value of assets under restraint was $178 million, and the value of assets under a court confiscation order, but not yet paid to the government, was $8.85 million, according to figures from the JFIU. It also reported that as of October 31, 2006, the amount confiscated and paid to the government since the enactment of DTRoP and OSCO was $55.4 million, and a total of 395 persons had been convicted of money laundering over that period. Hong Kong has shared confiscated assets with the United States.

In July 2002, the legislature passed several amendments to the DTRoP and OSCO to strengthen restraint and confiscation provisions. These changes, which became effective on January 1, 2003, include the following: there is no longer a requirement of actual notice to an absconded offender; there is no longer a requirement that the court fix a period of time in which a defendant is required to pay a confiscation judgment; the court is allowed to issue a restraining order against assets upon the arrest (rather than charging) of a person; the holder of property is required to produce documents and otherwise assist the government in assessing the value of the property; and an assumption is created under the DTRoP, to be consistent with OSCO, that property held within six years of the period of the violation by a person convicted of drug money laundering is proceeds from that money laundering.

Since legislation was adopted in 1994 mandating the filing of suspicious transaction reports (STRs), the number of STRs received by JFIU has generally increased. In the first nine months of 2006, a total of 10,782 STRs were filed, of which 1330 were referred to law enforcement agencies. This compares to a total of 13,505 STRs filed during all of 2005; 14,029 filed during 2004; and 11,671 during 2003. The JFIU plans to launch an electronic system for reporting STRs by registered users in late 2006.

The JFIU receives disclosures, conducts analysis, and in suitable cases distributes them to law enforcement investigating units. The JFIU can distribute cases to all Hong Kong law enforcement agencies, to similar overseas bodies and, in certain circumstances, to regulatory bodies in Hong Kong. The JFIU also conducts research on money laundering trends and methods, and provides case examples (typologies) to financial and nonfinancial institutions in order to assist them in identifying suspicious transactions. The JFIU has no regulatory responsibilities.

The Hong Kong Police has a number of dedicated units responsible for investigating financial crime, but the Commercial Crimes and Narcotics Bureaus in the Police Headquarters are the primary units responsible for investigating money laundering and terrorist financing.

The JFIU analyzes STRs to develop information that could aid in prosecuting money laundering cases, the number of which has also increased since 1996, soon after the passage of OSCO (1994). There were 44 prosecutions for money laundering during the first 9 months of 2006, compared to 40 for the entire year of 2004 and 29 for 2003. Hong Kong Customs had a significant money laundering case in 2006, in which the mastermind of a local pirated optical disc syndicate was convicted of money laundering involving HK$ 27.4 million ($3.5 million). These proceeds accrued over a four-year period from piracy activities. In July 2002, Hong Kong's legislature passed the United Nations (Anti-Terrorism Measures) Ordinance criminalizing supplying funds to terrorists. 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 that were in place in July 2004. It extends the Hong Kong Government's freezing power beyond funds to the nonfund property of terrorists and terrorist organizations. Furthermore, it prohibits 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.

The People's Republic of China (PRC) represents Hong Kong on defense and foreign policy matters, including UN affairs. After the PRC becomes a party to a UN terrorism treaty, the Hong Kong Government submits implementing legislation to Hong Kong's Legislative Council. After passage, the HKG executes the relevant UN treaty. 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. The PRC ratified the UN Convention against Corruption on 13 January 2006 and the UN Convention for the Suppression of the Financing of Terrorism on 19 April 2006.

To help deal with anti-money laundering (AML) issues from a practical perspective and reflect business needs, the Hong Kong Monetary Authority (HKMA) has recently coordinated the establishment of an Industry Working Group on AML, which includes representatives of some 20 authorized institutions. The Group has met twice, and three sub-groups have been established to share experiences and consider the way forward on issues such as PEPs (politically exposed persons), terrorist financing, transaction monitoring systems and private banking issues. The HKMA is also taking 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.

The HKMA circulated guidelines in 2004 incorporating the FATF Special Eight Recommendations on Terrorist Financing which require banks to maintain a database of terrorist names and management information systems to detect unusual patterns of activity in customer accounts. The Securities and Futures Commission (SFC) and the Office of the Commissioner of Insurance (OCI) circulated guidance notes in 2005 that provided additional guidance on customer due diligence and other issues, reflecting the new requirements in the Revised FATF Forty Recommendations on Money Laundering, and Special Recommendations on Terrorist Financing. The Hong Kong government has modified its regulations in order to make them consistent with the revised FATF Forty Recommendations on Money Laundering. In 2006, the OCI and the SFC revised their guidance notes to take into account the latest recommendations by the FATF.

Other bodies governing segments of the financial sector are also active in 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.

In 2003, Hong Kong took part in the International Monetary Fund's Financial Sector Assessment Program (FSAP), which aims to strengthen the financial stability of a jurisdiction by identifying the strengths and weaknesses of its financial system and assessing compliance with key international standards. As part of the FSAP, a team of IMF and World Bank-sponsored legal and financial experts assessed the effectiveness of Hong Kong's anti-money laundering regime against the FATF Forty Recommendations on Money Laundering and the FATF Special Recommendations on Terrorist Financing. The team described Hong Kong's anti-money laundering measures as "resilient, sound, and overseen by a comprehensive supervisory framework."

The Financial Investigations Division of the Narcotics Bureau has assisted the FBI in the investigation of the fugitives arrested in the United States in conjunction with the Bank of China case. In 2006, in a joint operation among the U.S. Immigration and Customs Enforcement (ICE), the U.S. Food and Drug Administration and Hong Kong Customs, a major mainland Chinese trafficker in counterfeit pharmaceutical drugs was identified. In September 2006, when the subject of the investigation arrived at a meeting in Hong Kong arranged by undercover agents, he was arrested by Hong Kong Customs officers under the Fugitive Offenders Ordinance.

Through the PRC, Hong Kong is subject to the 1988 UN Drug Convention. It is an active member of the FATF and Offshore Group of Banking Supervisors and also a founding member of the Asia Pacific Group on Money Laundering (APG). 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 with the United States that came into force in January 2000.

Hong Kong has mutual legal assistance agreements with a total of 21 other jurisdictions: Australia, Canada, the United States, Italy, the Philippines, the Netherlands, Ukraine, Singapore, Portugal, Ireland, France, the United Kingdom, New Zealand, the Republic of Korea, Belgium, Switzerland, Denmark, Israel, Poland, Germany and Malaysia. Hong Kong has also signed surrender-of-fugitive-offenders agreements with 16 countries, and has signed Agreements for the transfer-of-sentenced-persons with eight countries, including the United States.

Hong Kong authorities exchange information on an informal basis with overseas counterparts, with Interpol, and with Hong Kong-based liaison officers of overseas law enforcement agencies. An amendment to the Banking Ordinance in 1999 allows the HKMA to disclose information to an overseas supervisory authority about individual customers, subject to conditions regarding data protection. The HKMA has entered into memoranda of understanding with overseas supervisory authorities of banks for the exchange of supervisory information and cooperation, including on-site examinations of banks operating in the host country.

The Government of Hong Kong should further strengthen its anti-money laundering regime by establishing threshold reporting requirements for currency transactions and putting into place "structuring" provisions to counter evasion efforts. Per FATF Special Recommendation Nine, Hong Kong should also establish mandatory cross-border currency reporting requirements. Hong Kong should continue to encourage more suspicious transaction reporting by lawyers and accountants, as well as by business establishments such as auto dealerships, real estate companies, and jewelry stores. 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. Particularly since Hong Kong is a major trading center, Hong Kong law enforcement and customs authorities should seek to identify trade-based money laundering.

Hungary

Taking advantage of its pivotal location in central Europe, its cash-based economy and its well-developed financial services industry, criminal organizations from countries such as Russia and Ukraine have reportedly entrenched themselves in Hungary. Money laundering is related to a variety of criminal activities, including narcotics, prostitution, trafficking in persons, and organized crime. Additional financial crimes such as counterfeiting of euros, real estate fraud, and the copying/theft of bankcards are also prevalent. Financial crime has not increased in recent years, though there have been some isolated, albeit well-publicized, cases.

Hungary has been continuously improving its money laundering enforcement regime following its 2003 removal from the Financial Action Task Force (FATF) list of noncooperative countries and territories. Since then, it has worked to implement the FATF Forty Recommendations and the Nine Special Recommendations on Terrorist Financing. In early 2005, the International Monetary Fund (IMF), in conjunction with the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), conducted the third-round mutual evaluation of Hungary's anti-money laundering and counterterrorism financing regime. The evaluation team published the results of their assessment in June 2005.

Reacting to the advice cited in the mutual evaluation report, Hungary adopted an Action Plan and a new draft Anti-Money Laundering Act (AMLA) that will be submitted to the Parliament in September 2007. The draft AMLA addresses several (but not all) of the deficiencies cited in the mutual evaluation report. The draft law brings Hungary into compliance with the Vienna and Palermo Conventions by enlarging the scope of the money laundering offense so that it covers the transfer of proceeds to a third party even if it is carried out through a nonbanking or nonfinancial transaction. The draft AMLA also addresses reporting problems within Hungary's AML reporting system. According to the evaluation report, harsh criminal penalties for nonreporting have resulted in over filing by Hungarian financial institutions which are producing a high volume of suspicious transaction reports (STRs)—but which are of low quality. The draft law reduces the maximum punishment for the intentional failure to comply with reporting obligations from three years imprisonment to two years imprisonment. The maximum penalty for negligence in reporting has likewise been reduced from two years imprisonment to one year imprisonment, community service, or fine. Currently, the Hungarian Criminal Code only criminalizes terrorist acts committed by a group. The draft AMLA will include provisions punishing

the financing of terrorist acts which are committed by an individual. The draft law also establishes a clear legal basis for the obligation to report suspicious transactions relating to the financing of terrorism.

The AMLA also addresses FATF Special Recommendation Nine regarding cash couriers by requiring the declaration to Customs authorities of all movements of cash exceeding 10,000 euros (approximately $13,000). The draft law also calls for the establishment of an electronic database for the managing and processing of data contained in the Customs declarations.

Hungary banned offshore financial centers by Act CXII of 1996 on Credit Institutions. Offshore casinos are also prohibited from operating by the 1996 Act. At one time, there were offshore companies registered in Hungary that enjoyed a preferential tax benefits. However, the preferential tax treatment was phased out at the end of 2005 and in 2006, these companies were converted automatically into 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.

Hungary's first enacted anti-money laundering legislation in 1994 with Act XXIV. Hungary's money laundering legislation covers all serious crimes punishable by imprisonment. In April 2002, Section 303 of the Penal Code on Money Laundering was amended to criminalize self- laundering. In 2003, the Government of Hungary (GOH) re-codified its money laundering legislation in Act XV of 2003, "On the Prevention and Impeding of Money Laundering," which became effective on June 16, 2003. The 2003 Act extends the anti-money laundering legislation to encompass the following additional professions and business sectors: financial services, investment services, insurance, stock brokers, postal money transfers, real estate agents, auditors, accountants, tax advisors, gambling casinos, traders of gems or other precious metals, private voluntary pension funds, lawyers, and public notaries. Act XV also criminalizes tipping off and forces self-regulating professions to submit internal rules to identify asset holders, track transactions, and report suspicious transactions.

Hungary's financial regulatory body, the Hungarian Financial Supervisory Authority (HFSA), is charged with supervising financial service providers with the exception of cash processors, which are supervised by the National Bank of Hungary. Most designated nonfinancial businesses and professions (DNFBP) such as auditors, casinos, lawyers, and notaries are supervised by their own trade associations. Either the Hungarian National Police (HNP) or the Financial Intelligence Unit (FIU) within the HNP acts as the regulator for all other entities that are covered under the 2003 Act and that have no formal supervisory authority. In 2005, the HFSA conducted 169 on-site AML compliance inspections and issued enforcement warnings in 62 cases. In 2006, the HFSA established a new department specializing in issues pertaining to money laundering and financial crimes. That department is responsible for the coordination of supervisory tasks and duties related to money laundering and terrorist financing, and also assists other departments of the HFSA with on-site inspections.

The 2003 Act also states that covered service providers are required to identify their customers, or any authorized individual representing their customers, when entering into a business relationship. In transactions exceeding two million HUF (approximately $10,300) or transactions of any amount where suspicion of money laundering arises, the customer must be identified. Under the anti-money laundering legislation, banks, financial institutions, and other service providers are required to maintain records for at least ten years. All service providers are required to report suspicious transactions directly, or through their representation bodies, to the police authority as soon as they occur. Lawyers and notaries are obliged to file reports, except when they are representing their clients in a criminal court case. Both lawyers and notaries submit their reports to their respective bar and notary associations, which then forward the reports on to the police. All other service providers submit their reports directly to the police. The police may randomly perform on-site checks of service

providers. According to Hungarian bank secrecy regulations, financial service providers are obliged to supply law enforcement authorities with relevant data.

Safe harbor provisions protect individuals when executing their anti-money laundering reporting obligations. If the report involves suspicious activity related to terrorist financing, the law allows for the possibility of protection. Currently, however, actual extension of protection is granted at the discretion of the prosecutor.

As of 2001, only banks or their authorized agents can operate currency exchange booths. There are currently approximately 300 exchange booths in Hungary. These exchange booths are subject to "double supervision," because they are subject to the banks' internal control mechanisms, which are in turn subject to supervision by the HFSA. Exchange booths must verify customer identity for currency exchange transactions totaling or exceeding HUF 300,000 (approximately $1,500). These amounts can derive either from a single transaction or consecutive separate transactions which, in sum, exceeds this threshold. The exchange booths are also required to file suspicious transaction reports (STRs) for questionable currency exchange transactions in any amount. Monitoring of these suspicious transactions has resulted in ongoing criminal investigations.

Act CXX of 2001 eliminated bearer shares and required that all such shares be transferred to identifiable shares by the end of 2003. All shares now are subject to transparency requirements, and both owners and beneficiaries must be registered. By mid-2003, Hungary had successfully transferred 90 percent of anonymous savings accounts into identifiable accounts. Individuals must now have written permission from the police in order to access them.

Hungary's Financial intelligence Unit (FIU) is an investigative FIU and is part of the HNP. It investigates money laundering cases and has considerable authority to request and release information, both domestically and internationally. In the summer of 2004, the HNP completed a major organizational restructuring that included the establishment of the National Bureau of Investigation (NBI). The NBI is responsible for the detection and investigation of major corruption and money laundering cases. This restructuring has eliminated the parallel jurisdictions that existed in economic and financial crime investigations, and implemented a more coordinated investigative effort for money laundering investigations. The NBI houses the resulting new division, the Economic and Financial Crimes Department. The NBI has a staff of 134 at the headquarters level.

The FIU receives and investigates suspicious transaction information. In the first six months of 2006, the FIU received 5,195 STRs, opened 5,197 cases, and referred twenty of these cases to prosecutors. Banks filed the majority of these reports (80 percent), as well as currency exchange houses (16 percent). The 2005 Action Plan requires an impact study to review the supervision of these sectors, and aims to create programs to improve supervision and provide increased outreach and guidance to DNFBP's with regard to reporting obligations. Currently all obligated entities file reports using a paper system. However, the FIU is currently developing and testing a new electronic reporting system. During the first six months of 2006, a total of 20 money laundering investigations, involving 26 individuals had been opened. Five of these cases (14 persons) have reached the prosecution stage and are awaiting final judgments.

The Hungarian Criminal Code, Act XIX of 1998, and amended by Act II of 2003, contains a provision on the forfeiture of assets. Under this provision, assets that were used to commit crimes, would endanger public safety, or were created as a result of criminal activity, are subject to forfeiture. All property related to criminal activity during the period of time when the owner was a party to a criminal organization can be seized, unless proven to have been obtained in good faith as due compensation. Act II of 2003 states that persons or members of criminal organizations sponsoring activities of a terrorist group by providing material assets or any other support face five to fifteen years of imprisonment.

For most crimes, with the exception of terrorism financing, the police (including the FIU) freeze the assets and must then inform the bank within 24 hours as to whether there will be an investigation. Police investigations must be completed within two years of filing charges. Forfeiture and seizure for all crimes, including terrorist financing, is determined by a court ruling. The banking community has cooperated fully with enforcement efforts to trace funds and seize/freeze bank accounts. In all cases, some of the frozen assets may be released, for example, to cover health-related expenses or basic sustenance, if the FIU approves a written request from the owner of the assets. After subtracting any related civil damages, proceeds from asset seizures and forfeitures go to the government. In the first half of 2006, authorities seized assets in two money laundering cases worth a total of approximately 435,000 euro ($563,000).

Act IV of 1978, Article 261, criminalizes terrorist acts. Hungary has criminalized terrorism and all forms of terrorism financing with Act II of 2003, which modifies Criminal Code Article 261. The offense includes providing or collecting funds for terrorist actions or facilitating or supporting such actions by any means. The penalty for such crimes is imprisonment of five to fifteen years. The Hungarian Criminal Code does not include a separate provision for the financing of a terrorist act conducted by an individual. The FIU reported that only two of the STRs filed in 2006 were related to the financing of terrorism, in part because Hungary's current AML law does not provide a solid legal basis for an obligation to report suspicious financial activity related to terrorism financing. The draft AMLA contains provisions to correct these legal deficiencies.

The Hungarian Criminal Code treats terrorist financing-related crimes differently than all other crimes. Hungary can freeze terrorist finance-related assets. Act XIX of 1998 on Criminal Procedures, Articles 151, 159, and 160, provide for the immediate seizure, sequestration, and precautionary measures against terrorist assets. In cases where terrorist financing is suspected, banks freeze the assets and then promptly notify HFSA, the FIU, and the Ministry of Finance. The FIU must inform the banks within 24 hours whether or not it will conduct an investigation. The GOH circulates to its 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 E.O. 13224. Act CXII of 1996 on Credit Institutions bans the use of any indigenous alternative remittance systems that bypass, in whole or in part, financial institutions. In cases where money is transferred to a charitable or nonprofit entity, the GOH will freeze the assets regardless of the amount.

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.

Hungary is a member of the Council of Europe's MONEYVAL. Hungary's FIU has been a member of the Egmont Group since 1998.

Hungary is a party to the UN International Convention for the Suppression of the Financing of Terrorism; 1988 UN Drug Convention; and the UN Convention against Corruption. In December 2006 Hungary ratified the UN Convention against Transnational Organized Crime.

Hungary has made progress in developing its anti-money laundering regime. However, the GOH needs to continue its efforts with regard to implementation. An increased level of cooperation and coordination is needed among the different law enforcement entities involved in the anti-money laundering regime in Hungary. Prosecutors, judges, and police require additional training in order to promote the successful prosecution of money laundering cases. The HFSA and other supervisory bodies should improve supervision and provide increased outreach and guidance to financial

institutions with regard to reporting obligations. The GOH should take steps to ensure that nonbank financial institutions file suspicious transactions reports. Increased AML/CTF training for the employees of financial institutions and other obliged entities is also necessary in order to improve the number and quality of STRs filed, in particular those which may be related to the financing of terrorism. The FIU should continue work on the electronic reporting system until it is operational, and implement it. The GOH should enact the draft AMLA in September 2007 to ensure that Hungary comports with international standards, including those relating to the financing of terrorism.

India

India's growing status as a regional financial center, its large system of informal cross-border money flows, and its widely perceived tax avoidance problems all contribute to the country's vulnerability to money laundering activities. Some common sources of illegal proceeds in India are narcotics trafficking, 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 has been a drug-transit country.

India's strict foreign-exchange laws and transaction reporting requirements, combined with the banking industry's due diligence policy, make it difficult for criminals to use banks or other financial institutions to launder money. Accordingly, large portions of illegal proceeds are laundered through the alternative remittance system called "hawala" or "hundi." The hawala market is estimated at anywhere between 30 and 40 percent of the formal market. Remittances to India reported through legal, formal channels in 2005-2006 amounted to $24 billion (reportedly the largest in the world).

Reportedly, many Indians do not trust banks and prefer to avoid the lengthy paperwork required to complete a money transfer through a financial institution. The hawala system can provide the same remittance service as a bank with little or no documentation and at lower rates and provide anonymity and security for their customers. The Government of India (GOI) neither regulates hawala dealers nor requires them to register with the government. The Reserve Bank of India (RBI), the country's Central Bank, argues that the widespread hawala dealers operate illegally and therefore cannot be registered and are beyond the reach of regulation. Reportedly, the RBI does intend to increase its regulation of nonbank money transfer operations by entities such as currency exchange kiosks and wire transfer services.

Historically, gold has been one of the most important commodities involved in Indian hawala transactions. There is a widespread cultural demand for gold in the region. India liberalized its gold trade restrictions in the mid-1990s. In recent years, many believe the growing Indian diamond trade has also been increasingly important in providing countervaluation, a method of "balancing the books" in external hawala transactions. Invoice manipulation is used extensively to avoid both customs duties, taxes and to launder illicit proceeds through trade-based money laundering.

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 and an increase in the number of foreign companies doing business in India, the business volume in smuggled goods has fallen significantly. Most products previously sold in the black market are now traded through lawful channels.

While tax evasion is also widespread, 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 value added tax (VAT) in April 2005 which replaced numerous complicated state sales taxes and excise taxes. As a result, the

incentives and opportunities for businesses to conceal their sales or income levels have been reduced. Most of the twenty-eight Indian states have implemented the national VAT mandate, and the GOI anticipates that all states will be compliant by April 2007.

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 Narcotic Drugs and Psychotropic Substances Act (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 Act (SAFEMA) also allows for the seizure and forfeiture of assets linked to Customs Act violations. The competent authority (CA), located in the Ministry of Finance (MOF), administers both the NDPSA and the SAFEMA.

2001 Amendments to the NDPSA allow the CA to seize any asset owned or used by a narcotics trafficker immediately upon arrest. Previously, assets could only be seized after a conviction. Even so, Indian law enforcement officers lack training in 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 training 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 with India, the CA held nine asset seizure and forfeiture workshops in New Delhi, Himachal Pradesh, Uttar Pradesh, Rajasthan, and Andra Pradesh to train law enforcement officers in asset seizure and forfeiture procedures and regulations. The GOI hopes the training will lead to increased seizures and forfeitures from illicit narcotics proceeds.

The Foreign Exchange Management Act (FEMA), implemented in 2000, is one of the GOI's primary tools for fighting money laundering. 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. A closely related piece of legislation 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 FEMA and COFEPOSA. The RBI also plays an active role in the regulation and supervision of foreign exchange transactions.

The Prevention of Money Laundering Act (PMLA) was signed into law in January 2003. This legislation criminalizes money laundering, establishes fines and sentences for money laundering offenses, imposes reporting and record keeping requirements on financial institutions, provides for the seizure and confiscation of criminal proceeds, and provides for the creation of a financial intelligence unit (FIU). Implementing rules and regulations for the PMLA were promulgated in July 2005. Penalties for offenses under the PMLA are severe and may include imprisonment for three to seven years and fines as high as $10,280. If the money laundering offense is related to a drug offense under the NDPSA, imprisonment can be extended to a maximum of ten years. The PMLA mandates that banks, financial institutions, and intermediaries (such as stock market brokers) maintain records of all cash transactions exceeding $21,740. However, to date, there have been no prosecutions or convictions under the PMLA.

With the notification of the PMLA in July 2005, a financial intelligence unit (FIU) was established in January 2006 with the mandate to combat money laundering and terrorist financing. The FIU is the central repository to receive process, analyze, and disseminate information from suspicious transaction reports (STRs) and general cash transaction reports from financial institutions, banking companies, and intermediaries. It acts independently to refer such cases to the appropriate enforcement agency. Since it was initiated, India's FIU has received about 450 STRs.

The FIU is also responsible for strengthening efforts amongst the intelligence, investigative, and law enforcement agencies towards reaching global standards to prevent money laundering and related crimes. The FIU reports directly to the Economic Intelligence Council, which is headed by the Finance Minister. Administratively, it falls under the supervision of MOF's Department of Revenue. The FIU is not a regulatory agency but is permitted to exchange information with foreign FIUs on the basis of reciprocity, mutual agreement, or critical threat information on a case-by-case basis. There have been approximately 20 such information exchanges since FIU's establishment. As an Egmont observer, India's exchange of information with foreign FIUs is limited whereas full membership enables access to a global framework of sharing and obtaining terrorism financing information.

The MOF's Enforcement Directorate is responsible for investigations and for the prosecution of money laundering cases. The GOI has established an Economic Intelligence Council (EIC) to enhance coordination among the various enforcement agencies and directorates in the MOF. The EIC provides a forum for enforcement agencies 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 EIC, there are eighteen regional economic committees in India. The Central Economic Intelligence Bureau (CEIB) functions as the secretariat for the EIC. The CEIB interacts with the National Security Council, the Intelligence Bureau, and the Ministry of Home Affairs on matters concerning national security and terrorism.

The FIU and the MOF are actively working to amend regulations in order to be compliant with international standards. At present, the PMLA does not include comprehensive provisions on terrorism financing. The MOF has organized a committee of the relevant departments and ministries to amend the PMLA, which are likely to be introduced in the July-August, 2007 parliamentary session. Amendments will include provisions to criminalize terrorism financing and incorporate most of the FATF recommended categories of offenses.

In October 2006, the Finance Ministry stated that India had agreed to reconcile its list of predicate crimes with that of the Financial Action Task Force (FATF) and not set minimum property value thresholds on predicate crimes. As of December 2006, India is a FATF observer and has a two year probationary period to become compliant with FATF norms to become a member. Full FATF membership has been one criterion identified to help India move towards a sufficient anti-money laundering and terrorist financing (AML/CTF) regime required by the U.S. Federal Reserve Board in making determinations on foreign bank branch applications. In this context, the GOI is seeking to amend the PMLA to block terrorism financing through banking and financial institution channels. After PMLA changes are fully enacted, the Securities and Exchange Board of India (SEBI) Act will also be revised to include similar offenses.

The Central Bureau of Investigation (CBI), the Directorate of Revenue Intelligence (DRI), Customs and Excise, RBI, the Competent Authority, and the MOF are all active in anti-money laundering efforts. During 2004, DRI referred four hawala-based money laundering cases with a U.S. nexus to the U.S. Department of Homeland Security/Immigration and Customs Enforcement (DHS/ICE). DHS/ICE carried out successful investigations on three of these cases and forwarded tangible results to the MOF's Department of Enforcement. During 2005, the Directorate of Enforcement (DOE) forwarded two additional hawala-linked money laundering cases to DHS/ICE. DHS/ICE has provided investigative assistance.

Many banking institutions, prompted by the RBI, have taken steps on their own to combat money laundering. For example, banks are beginning to hire compliance officers to ensure that anti-money laundering regulations are being observed. The RBI issued a notice in 2002 to commercial banks instructing them to adopt the due diligence rules. The Indian Bankers Association established a working group to develop self-regulatory anti-money laundering procedures. Foreign customers, applying for accounts in India must show proof of identity when opening a bank account. Banks also

require that the source of funds must be declared if the deposit is more than $10,000. Finally, banks must report suspicious transactions.

Since March 2006, the FIU has been receiving reports on suspicious transactions and cash flows from banks, financial institutions, and intermediaries involving over USD $22,490. About 50 percent of such transactions are reported electronically by public and private banks (led by the large private banks) while the other institutions are only equipped to report manually. The FIU is in the process of developing a secure gateway for submission of electronic STRs which should be in place by December 2007.

A circular to all intermediaries registered with SEBI was issued on the obligations to prevent money laundering. The circular included information on the maintenance of records, preservation of information with respect to certain transactions, and reporting to the Director of the FIU suspicious cash flows and financial transactions.

The GOI has the power to order banks to freeze assets. In November 2004, the RBI issued a circular updating its due diligence guidelines drafted to ensure that they comply with Financial Action Task Force (FATF) recommendations. The guidelines include the requirement that banks identify politically-connected account holders residing outside India and identify the source of funds before accepting deposits from these individuals. The UNSCR 1267 Sanctions Committee's consolidated list is routinely circulated to all financial institutions. The RBI also asked all commercial banks to become FATF-compliant in terms of customer identification for existing as well as new accounts. These guidelines went into effect in December 2005. Banks have been enforcing the guidelines strictly with new customers and gradually phasing in the procedures with old customers. High-risk accounts are subject to intense monitoring.

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.

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.

GOI regulations governing charities remain antiquated and the process by which charities are governed at the provincial and regional levels remain 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 remain no guidelines or provisions governing the oversight of charities for AML/CFT purposes, and there remains a need for increased integration between charities regulators and law enforcement authorities regarding the threat of terrorist finance. In April 2002, the Indian Parliament passed the Prevention of Terrorism Act (POTA), which criminalizes terrorist financing. In March 2003, the GOI announced that it had charged 32 terrorist groups under the POTA. In July 2003, the GOI announced that it had arrested 702 persons under the POTA. In November 2004, the Parliament repealed the POTA and amended the 1967 Unlawful Activities (Prevention) Act to include the POTA's salient elements such as criminalization of terrorist financing.

India is a party to the 1988 UN Drug Convention, and is a member of the Asia/Pacific Group (APG) on Money Laundering. India implements the 1988 UN Drug Convention through amendments to the

NDPSA (in 1989 and 2001) and the PMLA. It is a signatory to, but has not yet ratified, the UN Convention against Transnational Organized Crime. India is a party to the UN International Convention for the Suppression of the Financing of Terrorism. In October 2001, the GOI and the United States signed a mutual legal assistance treaty, which took effect in October 2005. India has also signed a police and security cooperation protocol with Turkey that provides for joint efforts to combat money laundering. The GOI is implementing this convention through the Unlawful Activities Prevention Act.

Since terrorist financing in India is linked to the hawala system, the Government of India should cooperate fully with international initiatives to provide increased transparency in alternative remittance systems, and, if necessary should initiate regulation and increase law enforcement actions in this area. India should examine the scope of its citizens' involvement in the illicit international diamond trade. It also needs to quickly finalize the implementation of regulations to the anti-money laundering law and ensure that the new FIU is fully operational. Meaningful tax reform will also assist in negating the popularity of hawala and lessen money laundering. Increased enforcement action should also be taken in order to effectively combat trade-based money laundering. Additionally, India should become a party to the UN Convention against Transnational Organized Crime.

Indonesia

Although neither a regional financial center nor an offshore financial haven, Indonesia is vulnerable to money laundering and terrorist financing due to a poorly regulated financial system, the lack of effective law enforcement, and widespread corruption. Most money laundering in the country is connected to nondrug criminal activity such as gambling, prostitution, bank fraud, piracy and counterfeiting, illegal logging, and corruption. Indonesia also has a long history of smuggling, a practice facilitated by thousands of miles of un-patrolled coastline and a law enforcement system riddled with corruption. The proceeds of these illicit activities are easily parked offshore and only repatriated as required for commercial and personal needs.

As a result of Indonesia's ongoing efforts to implement the reforms to its Anti-Money Laundering (AML) regime, the Financial Action Task Force (FATF) removed Indonesia from its list of Non-Cooperative Countries and Territories (NCCT) on February 11, 2005 and subsequent special FATF monitoring on February 11, 2006. The removal of Indonesia from the NCCT list and special monitoring recognized a concerted, interagency effort-supported by President Susilo Bambang Yudhoyono-to further develop Indonesia's nascent AML regime.

Indonesia's Financial Intelligent Unit (PPATK), established in December 2002 and fully functional since October 2003, continues to make steady progress in developing its human and institutional capacity. The PPATK is an independent agency that receives, analyzes, and evaluates currency and suspicious financial transactions, provides advice and assistance to relevant authorities, and issues publications. As of November 30, 2006 the PPATK has received approximately 6,884 suspicious transactions reports (STRs) from 115 banks and 47 nonbank financial institutions. The volume of STRs has increased from an average of 70 per month in 2004 to 324 per month in 2006. The agency also reported that it had received over 1.9 million cash transaction reports (CTRs). Based on their analysis of 608 STRs, PPATK investigators have referred 417 cases to the police. Based on referrals of STRs and other related information from the PPATK, there have been over 30 convictions for money laundering or its predicate crimes, including six for money laundering only. Of the six money laundering convictions, three were handed down in January and included sentences between five to seven years.

Indonesia's Anti-Money Laundering and Counter Terrorism Finance (CTF) Donors' Coordination Group, co-chaired by the PPATK and the Australian Agency for International Development (AUSAID), has become a model for AML/CTF donors' coordination groups in other countries. Since

Indonesia's removal form the NCCT list, donors and the Government of Indonesia (GOI) have placed greater emphasis on more practical training; technical and capacity-building assistance for the nonbank financial sector, police, prosecutors and judges; cash smuggling; and regulation of charities and money changers. In July 2006, the Asia Pacific Group (APG) named PPATK Chairman Yunus Husein a co-chair of the regional FATF style organization for a two-year term. In November 2006, Indonesia hosted the annual APG Typologies Workshop.

The PPATK is actively pursuing broader cooperation with relevant GOI agencies. The PPATK has signed ten 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 (Bapepam), the Ministry of Finance Directorate General of Financial Institutions, 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), and the Corruption Eradication Committee.

Sustained public awareness campaigns, new bank and financial institution disclosure requirements, and the PPATK's support for Indonesia's first credible anticorruption drive have led to increased public awareness about money laundering and, to a lesser degree, terrorism finance. However, weak human and technical capacity, poor interagency cooperation, and corruption, still remain significant impediments to the continuing development of an effective and credible AML regime.

Banks and other financial institutions now routinely question the sources of funds or require identification of depositors or beneficial owners. Financial reporting requirements were put in place in the wake of the 1998 Asian financial crisis when the GOI became interested in controlling capital flight and recovering foreign assets of large-scale corporate debtors or alleged corrupt officials.

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 PPATK to develop policy and regulations to combat money laundering and terrorist financing.

In September 2003, Parliament passed Law No. 25/2003 amending Law No. 15/2002 Concerning the Crime of Money Laundering in order to address many FATF concerns. Amending Law No. 25/2003 provides a new definition of 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 origins of the assets. The amendment removes the threshold requirement for proceeds of crime and expands the definition of proceeds of crime to cover assets employed in terrorist activities. The amendment expands the scope of regulations requiring STRs to include attempted or unfinished transactions. The amendment also shortens the time to file an STR to three days or less after the discovery of an indication of a suspicious transaction. The amendment makes it an offense to disclose information about the reported transactions to third parties, which carries a maximum of five years' imprisonment and a maximum of one billion rupiah (approximately $110,000). Articles 44 and 44A 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 GOI enacted Indonesia's first Mutual Legal Assistance (MLA) Law (No. 1/2006), establishing formal, binding procedures to facilitate MLA with other states.

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. Finally, the regulation requires banks to analyze and monitor customer transactions and report to BI within seven days any "suspicious transactions" in excess of Rp 100 million (approximately $11,000). The regulation defines suspicious transactions according to a 39-point matrix that includes key indicators such as unusual cash transactions, unusual ownership patterns, or unexplained changes in transactional behavior. BI specifically requires banks to treat as suspicious any transactions to or from countries "connected with the production, processing and/or market for drugs or terrorism."

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. 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. 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 Rupiah (approximately $11,000) 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. Indonesian 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, deposit of Indonesia Rupiah into or out of Indonesia. The Decree provides implementing guidance for Ministry of Finance Regulation No.624/PMK.04/2004 of December 31, 2004, and requires individuals who import or export more than rupiah 50 to 100 million in cash (approximately $5,500-$11,000) to report such transactions to Customs. This information is to be declared on the Indonesian Customs Declaration (BC2.2). As of October 2006, the PPATK has received more than 1,200 reports from Customs on cross border cash carrying issues. The reports came from five entry points as follows: Batam Port, Jakarta's Soekarno Hatta Airport, Tanjung Balai Karimun Port, Ngurah Rai Bali Airport, and Husein Sastranegara Bandung Airport.

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 now 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. Article 15 of the anti-money laundering legislation gives providers of financial services, their officials, and employees protection from civil or criminal action in making such disclosures.

Indonesia's laws provide only limited authority to block or seize assets. Under BI regulation 2/19/PBI/2000, police, prosecutors, or judges may order the seizure of assets of individuals or entities that have been either declared suspects or indicted for a crime. This does not require the permission of BI, but, in practice, for law enforcement agencies to identify such assets held in Indonesian banks, BI's permission is sought. In cases when money laundering is the alleged crime, however, bank secrecy laws would not apply, according to the anti-money laundering law.

The GOI has the authority to trace and freeze assets of individuals or entities on the UNSCR 1267 Sanctions Committee's consolidated list, and through BI, has circulated the consolidated list to all

banks operating in Indonesia, with instructions to freeze any such accounts. The interagency process to issue freeze orders, which includes the Foreign Ministry, Attorney General, Police, and BI, takes several weeks or more from UN designation to bank notification. The implementation of this process has not led to the discovery of accounts or assets of individuals or entities on the UN 1267 consolidated list. However, during the course of terrorism investigations, the Indonesia police have located and frozen accounts of individuals on the UN 1267 consolidated list.

In August, 2006, the GOI enacted Indonesia's first Witness and Victim Protection Law (No. 13/2006). Indonesia's AML Law and Government Implementing Regulation No. 57/2003 also provides protection to whistleblowers and witnesses.

In October 2006, the GOI submitted to Parliament additional amendments to Law No. 15/2002 that would provide the PPATK with preliminary investigative authority and the ability to temporarily freeze assets. The amendments are intended to provide technical investigative support to police and prosecutors and to deter capital flight.

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. 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. 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 GOI has just begun to take into account alternative remittance systems, such as charitable and nonprofit entities in its strategy to combat terrorist finance and money laundering. 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 GOI has initiated a dialogue with charities and nonprofit entities to enhance regulation and oversight of those sectors.

Indonesia is an active member of the Asia/Pacific Group on Money Laundering (APG) and the Bank for International Settlements. BI claims that it voluntarily follows the Basel Committee's "Core Principles for Effective Banking Supervision." The GOI is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. In June, 2006, Indonesia became a party to the UN International Convention for the Suppression of the Financing of Terrorism.

In June 2004, the PPATK became a member of the Egmont Group and, as such, is committed to the Group's established Principles governing the exchange of financial intelligence with other members. The PPATK is actively pursuing broader cooperation through the MOU process with approximately twenty other 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, and Indonesia joined other ASEAN nations in signing the ASEAN Treaty on Mutual Legal Assistance in Criminal Matters on November 29, 2004. 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 highest levels of GOI leadership should continue to demonstrate strong support for strengthening Indonesia's anti-money laundering regime. In particular, 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 and custodial and administrative sentences and penalties. As part of this effort, Indonesia should review the adequacy of its Code for Criminal Procedure and Rules of Evidence and enact legislation to allow the use of modern techniques to enter evidence in court proceedings. Indonesia should reassess and streamline its processes for reviewing UN designations and for identifying, freezing and seizing terrorist assets. The GOI should expand its list of predicate crimes for money laundering. Indonesia should also become a party to the UN Convention against Transnational Organized Crime.

Iran

Iran is not a regional financial center. Iran's economy is marked by an inefficient state sector, over-reliance on the petroleum industry—Iran's huge oil and gas reserves produce 60 percent of government revenue—and state-centered policies that cause major distortions in the economy. Reportedly, a prominent Iranian banking official estimates that money laundering encompasses an estimated 20 percent of Iran's economy. There are other reports that over $11 billion a year is laundered via smuggling commodities in Iran and over $6 billion is laundered by international criminal networks. The World Bank reports that about 19 percent of Iran's GDP pertains to unofficial economic activities. Money laundering in Iran encompasses narcotics trafficking, smuggling, trade fraud, counterfeit merchandise and intellectual property rights violations, cigarette smuggling, trafficking in persons, hawala, capital flight, and tax evasion.

After the Iranian Revolution of 1979, the Government of Iran (GOI) nationalized the country's banks, leaving a total of six banks: Bank Refah, Bank Melli Iran, Bank Saderat, Bank Tejarat, Bank Mellat and Bank Sepah, and three specialized institutions, Bank Keshavrzi, Bank Maskan and Bank Sanat va Madden. No foreign banks were allowed to operate in the country. Since 1983, consistent with Islamic law, banks have been prohibited from paying interest on deposits or charging interest on loans. However, alternative financial instruments were developed including profit-sharing and financing based on trade. In 1994, Iran authorized the creation of private credit institutions. Licenses for these banks were first granted in 2001. Currently, these banks include Larafarinan, Parsian, Saman Eghtesad and Eghtesade Novin. Standard Chartered Bank became the first foreign bank to be awarded a license to establish a branch in Iran, although this was limited to Kish, a free-zone island. Currently, some 40 international banks have representative offices in Iran, which may undertake lending but not accept deposits.

There are currently no meaningful anti-money laundering (AML) controls on the Iranian banking system. The Central Bank of Iran (CBI) has issued AML circulars that address suspicious activity reporting and other procedures that demonstrate an awareness of international standards, but there is a lack of implementation. In 2003, the Majlis (Parliament) reportedly passed an anti-money laundering act. The act includes customer identification requirements, mandatory record keeping for five years after the opening of accounts, and the reporting of suspicious activities. However, the act has not been implemented due to reported pressure by vested interests within the government.

Iran has reported to the United Nations that it has established a financial intelligence unit (FIU). However, Iran has not provided any documentation or details on the FIU.

The U.S. Department of State has designated Iran as a State Sponsor of Terrorism. On September 8, 2006 the U.S. Treasury Department issued a regulation prohibiting U.S. financial institutions from handling any assets, directly or indirectly, relating to Iran's Bank Saderat, based on evidence of its involvement in transferring funds to terrorist groups. Bank Saderat is one of Iran's largest with approximately 3,400 branches.

On January 9, 2007, the U.S. Treasury Department imposed sanctions against Bank Sepah, a state-owned Iranian financial institution for providing support and services to designated Iranian

proliferation firms, particularly Iran's missile procurement network. Bank Sepah is the fifth largest Iranian state-owned bank with more than 290 domestic branches as well as international branches in Europe.

Iran has a very large underground economy, which is spurred by restrictive taxation, widespread smuggling, currency exchange controls, capital flight, and a large Iranian expatriate community. Anyone engaging in transfers or transactions of foreign currency into or out of Iran must abide by CBI regulations, including registration and licensing. Those who do not are subject to temporary or permanent closure. The regulations and circulars address money transfer businesses, including hawaladars. However, underground hawala and moneylenders in the bazaar are active in Iran. Since there is an absence of an adequate banking system and working capital, the popular informal system meets the need for currency exchange and money lending. Many hawaladars and traditional bazaari are linked directly to the regional hawala hub in Dubai. Countervaluation in hawala transactions is often accomplished via trade. The trade and smuggling of goods into Iranian commerce leads to a significant amount of trade-based money laundering and value transfer.

Iran's real estate market is often used to launder money. Often times, 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.

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. There are reports that the transit trade facilitates the laundering of Afghan narcotics proceeds. 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 3 million drug users and the worst 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.

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 Iranian import-export concerns and 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 entrepreneurs not affiliated with them due to the bonyads' favored status, which includes exemption from taxes, the granting of favorable exchange rates, and lack of accounting oversight by the Iranian government. Corruption is widespread throughout Iranian society; at the highest levels of government, favored individuals and families benefit from "baksheesh" deals. Iran is ranked 106 out of 163 countries listed in Transparency International's 2006 Corruption Perception Index. Despite some limited attempts at reforming bonyads, there has been little transparency or substantive progress. Bonyads have been involved in funding terrorist organizations and serving as fronts for the procurement of nuclear capacity and prohibited weapons and technology.

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

The Government of Iran should construct and implement a viable anti-money laundering and terrorist finance regime that adheres to international standards. 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 anti-corruption law with strict penalties and enforcement, applying it equally to figures with close ties to the government and the clerical communities. It should ratify the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. Iran should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism. Iran should not support terrorism or the funding of terrorism.

Iraq

Iraq's economy is cash-based. There is little data available on the extent of money laundering in Iraq. However, cross-border smuggling is widespread, including the smuggling of bulk cash. Iraq is a major market for smuggled cigarettes and counterfeit goods, and money is laundered from intellectual property right violations. There is a large market for stolen cars from Europe and the United States. Ransoms generated from kidnapping generate tens of millions of dollars every year. Kidnappings are linked to human exploitation and terrorist finance. Iraq is a source country for human trafficking. Trade-based money laundering, customs fraud, and value transfer are found in the underground economy and are commonly used in informal value transfer systems such as hawala. Hawala networks are prevalent and are widely used in Iraq and the region. Cash, trade-based money laundering, and hawala are all components of terrorist and insurgent finance found in Iraq. In early 2006, the Iraqi oil ministry estimated that ten percent of the $4 billion to $5 billion in fuel imported for public consumption at subsidized rates in 2005 was smuggled internally and out of the country for resale at market rates. Moreover, there are reports that approximately ten percent of all oil smuggling profits are going to insurgents. Subsidy scams and black market sales also exist for gasoline, kerosene, and cooking fuel. Corruption is a severe problem that permeates society and commerce and is also found at the highest levels of government and other institutions. Transparency International's 2006 International Corruption Perception Index listed Iraq 161 out of 163 countries surveyed. The formal financial sector is growing and at least ten new banks, both domestic and international, have been licensed to operate in Iraq. The two state-owned banks control at least 90 percent of the banking sector.

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.

The CPA Order No. 93, "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 in regard to financial transactions. The law also criminalizes money laundering, financing crime (including the financing of terrorism), and structuring 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 required to verify the identity of any customer opening an account for any amount. Covered entities are also required to verify the identity of non-account holders performing a transaction or series of potentially related transactions whose value is equal to or greater than five