## Isle of Man

The Isle of Man (IOM) is a Crown Dependency of the United Kingdom with its own parliament, government, and laws. Its large and sophisticated financial center is potentially vulnerable to money laundering at the layering and integration stages. Most of the illicit funds in the IOM are from fraud schemes and narcotics trafficking in other jurisdictions, including the United Kingdom. The U.S. dollar is the most common currency used for criminal activity in the IOM. Identity theft and Internet abuse are growing segments of financial crime activity.

No current data regarding the entities that comprise the IOM financial industry has been reported. As of September 30, 2004, the IOM's financial industry consisted of approximately 19 life insurance companies, 25 insurance managers, more than 177 captive insurance companies, 53 licensed banks and two licensed building societies, 82 investment business license holders, 30.1 billion pounds (approximately U.S. $59 billion) in bank deposits, and 164 collective investment schemes with 6.5 billion pounds (approximately U.S. $12.7 billion) of funds under management. There were also 171 licensed corporate service providers.

The IOM criminalized money laundering related to narcotics trafficking in 1987. The Criminal Justice (Money Laundering Offenses) Act 1998, extends the definition of money laundering to cover all serious crimes and led to the creation of the Anti-Money Laundering (AML) Code, which came into force in December 1998. The AML Code has subsequently been replaced by the Criminal Justice (Money Laundering) Code 2007 (the Code), enacted in September 2007. Requirements under the 2007 Code apply to banking, investment, and collective investment schemes, fiduciary services business, insurance, building societies, credit unions, local authorities authorized to raise or borrow money, bureaux de change, estate agents, bookmakers and casinos (excluding online gambling), accountants, notaries and legal practitioners, insurance intermediaries, retirement benefits schemes, administrators and trustees, auditors, the Post Office, and any activity involving money transmission services or check encashment facilities.

The Code requires that obligated entities implement AML policies, procedures, and practices, including employing them for countering terrorist financing. The Code mandates that obligated entities institute procedures to establish customer identification requirements; report suspicious transactions; maintain adequate records; adopt adequate internal controls and communication procedures; provide appropriate training for employees; and establish internal reporting protocols. There is no minimum threshold for obliged entities to file a suspicious transaction report (STR), and safe harbor provisions in the law protect reporting individuals when they file an STR. It is an offense to fail to disclose suspicion of money laundering for all predicate crimes. Failure to comply with the requirements of the Code may bring a fine, imprisonment of up to two years, or both.

The Financial Supervision Commission (FSC) and the Insurance and Pension Authority (IPA) regulate the IOM financial sector. The IPA regulates insurance companies, insurance management companies, general insurance intermediaries, and retirement benefit schemes and their administrators. The FSC is responsible for the licensing, authorization, and supervision of banks, building societies, investment businesses, collective investment schemes, corporate service providers, and companies. The FSC also maintains the Company Registry Database for the IOM, which contains company records dating back to the first company incorporated in 1865. Statutory documents filed by IOM companies can now be searched and purchased online through the FSC's website.

As IOM's companion to the AML Code, the FSC has AML Guidance Notes (AMLGN), which the FSC rewrote in 2007. The new guidance reflects evolving international standards, new legislation on the Island, and the new licensee status of Corporate Service Providers and Trust Service Providers. In 2008, the FSC will release the new revised guidance as an "Anti-Money Laundering and the Financing of Terrorism Handbook."

The FSC has worked with its counterparts from the Crown Dependencies of Guernsey and Jersey. One of these initiatives was a consultation paper called Overriding Principles for a Revised Know Your Customer (KYC) Framework, to develop a more coordinated AML approach. Work between the Crown Dependencies is continuing, to develop a coordinated strategy on money laundering, and to ensure maximum compliance with the revised Financial Action Task Force (FATF) Forty Recommendations on Money Laundering.

Money service businesses (MSBs) not already regulated by the FSC or IPA must register with Customs and Excise. With this, the IOM implemented the first two EU Directives on Money Laundering, and provides for their supervision by Customs and Excise to ensure compliance with the AML Code. In December 2007, the FSC issued a Consultative Paper on the Proposed Regulation of MSBs, including electronic money (e-money) providers. This document will assist the Island in meeting the standards set by the Financial Action Task Force ("FATF") 40 Recommendations and Nine Special Recommendations on Terrorist Financing. The paper also airs proposals to bring money MSBs and e-money providers under some form of regulation, which would initially be limited.

The IPA, as regulator of the IOM's insurance and pensions business, issues Anti-Money Laundering Standards for Insurance Businesses (the "Standards"). The Standards are binding upon the industry and include "Overriding Principles" requiring all insurance businesses to check their businesses to determine that they have sufficient information available to prove customer identity. The current set of Standards became effective March 31, 2003. The IPA conducts on-site visits to examine procedures and policies of companies under its supervision.

The Online Gambling Regulation Act 2001 and an accompanying AML (Online Gambling) Code 2002 are supplemented by AML guidance notes issued by the Gambling Control Commission, a regulatory body which provides guidance on the prevention of money laundering in the online gaming sector. The Online Gambling legislation, unique to the gaming industry when it passed, brought regulation to an unregulated gaming environment. The revised version of the Online Gambling and Peer to Peer Gambling AML Code came into force in 2006.

The Companies, Etc. (Amendment) Act 2003 provides for additional supervision for all licensable businesses, e.g., banking, investment, insurance, and corporate service providers. The act abolished future bearer shares after April 1, 2004, and mandates that all existing bearer shares be registered before the bearer can exercise any rights relating to the shares.

The Financial Crime Unit (FCU), under the Department of Home Affairs, the intelligence financial unit (FIU) of the Isle of Man, was formed in April 2000 and evolved from the police Fraud Squad. It is the central point for the collection, analysis, investigation, and dissemination of suspicious transaction reports (STRs) from obligated entities. The FCU's work is broadly split between financial intelligence, legal co-operation with other jurisdictions in terms of financial investigation, and local financial crime investigation involving serious or complex cases. It is comprised of Police and Customs Officers, Police Support Staff, and other government departments such as Internal Audit and HM Attorney General's Chambers. The FIU has access to Customs, police, and tax information. The FIU disseminates STRs to the Customs, Tax Administrators, FSC, and the IPA. The FCU is responsible for investigating financial crimes and terrorist financing cases. The FIU received approximately 1,574 suspicious transaction reports in 2007, and 1,653 STRs in 2006. Approximately 45 percent of the STRs are disseminated to the United Kingdom, five percent to other European countries, and seven percent to nonEuropean countries (mainly the U.S.). IOM authorities charged eight people with money laundering offenses in 2007, and investigations are proceeding. Six of the eight have been charged in relation to narcotics, and two to fraud, including wire fraud. In 2006, IOM authorities obtained one conviction for money laundering.

IOM legislation provides powers to constables, including customs officers, to investigate whether a person has benefited from any criminal conduct. These powers allow information to be obtained about

that person's financial affairs. These powers can be used to assist in criminal investigations abroad as well as in the IOM. The Customs and Excise (Amendment) Act 2001 gives various law enforcement and statutory bodies within the IOM the ability to exchange information, where such information would assist them in discharging their functions. The Act also permits Customs and Excise to release information it holds to any agency within or outside the IOM for the purposes of any criminal investigation and proceeding. Such exchanges can be either spontaneous or by request.

The Criminal Justice Acts of 1990 and 1991, as amended, extend the power to freeze and confiscate assets to a wider range of crimes, increase the penalties for a breach of money laundering codes, and repeal the requirement for the Attorney General's consent prior to disclosure of certain information. The law also lowers the standard for seizing cash from "reasonable grounds" to believe that it was related to drug or terrorism crimes to a "suspicion" of any criminal conduct. Assistance by way of restraint and confiscation of a defendant's assets is available under the 1990 Act to all countries and territories designated by Order under the Act. Assistance is also available under the 1991 Act to all countries and territories in the form of the provision of evidence for the purposes of criminal investigations and proceedings. The availability of such assistance is not convention-based nor does it require reciprocity.

All charities operating within the IOM are registered and supervised by the Charities Commission.

The Prevention of Terrorism Act 1990 made it an offense to contribute to terrorist organizations or to assist a terrorist organization in the retention or control of terrorist funds. The IOM Terrorism (United Nations Measure) Order 2001 implements UNSCR 1373 by providing for the freezing of terrorist funds, as well as by criminalizing the facilitating or financing of terrorism. The Government of the IOM enacted the Anti-Terrorism and Crime Act, 2003, which enhances reporting by making the failure to report suspicious transactions relating to money intended to finance terrorism an offense. All other UN and EU financial sanctions have been adopted or applied in the IOM, and are administered by Customs and Excise. Institutions are obliged to freeze affected funds and report the facts to Customs and Excise. In December 2001, the FSC issued revised AML guidance notes that include information relevant to terrorism. IOM authorities are reviewing additional amendments that will incorporate the most recent FATF recommendations and EU directives.

The IOM has developed a legal and constitutional framework for combating money laundering and the financing of terrorism. In 2003, the International Monetary Fund (IMF) examined the regulation and supervision of the IOM's financial sector and found that "the financial regulatory and supervisory system of the Isle of Man complies well with the assessed international standards."

Application of the 1988 UN Drug Convention was extended to the IOM in 1993. In 2003, the U.S. and the UK agreed to extend to the Isle of Man the U.S.-UK Treaty on Mutual Legal Assistance in Criminal Matters.

The IOM cooperates with international anti-money laundering authorities on regulatory and criminal matters. Under the 1990 Criminal Justice Act, the provision of documents and information is available to all countries and territories for the purposes of investigations into serious or complex fraud. Similar assistance is also available to all countries and territories in relation to drug-trafficking and terrorist investigations. All decisions for assistance are made by the Attorney General of the IOM on a case-by-case basis, depending on the circumstances of the inquiry.

In October 2007, the IOM signed tax information exchange agreements (TIEAs) with each member of the Nordic Council (Denmark, the Faroe Islands, Finland, Greenland, Iceland, Norway, and Sweden) and received commendation from the Organization for Economic Co-operation and Development for its commitment to international standards. The IOM has a fully operational TIEA with the United States and has established protocols with the Internal Revenue Service (IRS) to ensure that information exchange requests are handled smoothly.

Although not a member of the FATF, the Island fully endorses FATF 40 Recommendations and Nine Special Recommendations. The IOM's experts are assisting the FATF working group that considers matters relating to customer identification and companies' issues. The IOM is a member of the Offshore Group of Banking Supervisors (OGBS) and Offshore Group of Insurance Supervisors (OGIS). The FCU belongs to the Egmont Group.

Isle of Man officials should continue to support and educate the local financial sector to help it combat current trends in money laundering. The IOM should act on the 2007 Consultative paper with the MSB/e-money regulation proposals that authorities have discussed, and implement the most effective. The IOM should also ensure that the obliged entities understand and respond to their new and revised responsibilities as delineated by the 2007 AML Code. To this end, the FSC should work to release the Anti-Money Laundering and Terrorist Financing Handbook as soon as possible in 2008. The authorities also should continue to work with international AML authorities to deter financial crime and the financing of terrorism and terrorists.

## Israel

Among its Mediterranean neighbors, Israel stands out economically in terms of its high GDP, per capita income, developed financial markets and diverse capital markets. Nevertheless, Israel is not regarded as a regional financial center. It primarily conducts financial activity with the financial markets of the United States and Europe, and to a lesser extent with the Far East. Israeli National Police (INP) intelligence identifies illicit drugs, gambling, extortion, and fraud as the predicate offenses most closely associated with organized criminal activity. Recent studies conducted by the INP Research Department estimate illegal gambling profits at U.S. $2-3 billion per year and domestic narcotics profits at U.S. $1.5 billion per year. Human trafficking is considered the crime-for-profit with the greatest human toll in Israel, and public corruption the crime with the greatest social toll. As such, these areas are the targets of the most vigorous anti-money laundering (AML) enforcement activity. Israel does not have free trade zones and is not considered an offshore financial center, as offshore banks and other forms of exempt or shell companies are not permitted. Bearer shares, however, are permitted for banks and/or for companies.

In August 2000, Israel enacted its anti-money laundering legislation, the "Prohibition on Money Laundering Law" (PMLL), (Law No. 5760-2000). The PMLL established a framework for an anti-money laundering system, but required the passage of several implementing regulations before the law could fully take effect. Among other things, the PMLL criminalized money laundering and included 18 serious crimes, in addition to offenses described in the prevention of terrorism ordinance, as predicate offenses for money laundering even if committed in a foreign jurisdiction.

The PMLL also provided for the establishment of the Israeli Money Laundering Prohibition Authority (IMPA) under the Ministry of Justice, as the country's financial intelligence unit (FIU). IMPA became operational in 2002. The PMLL requires financial institutions to report "unusual transactions" to IMPA as soon as possible under the circumstances. Financial institutions must report all transactions that exceed a minimum threshold that varies based on the relevant sectors and the risks that may arise, with more stringent requirements for transactions originating in a high-risk country or territory. IMPA has access to population registration databases, the Real-Estate Database, records of inspections at border crossings, court files, and Israel's Company Registrar.

In 2001, Israel adopted the Banking Corporations Requirement Regarding Identification, Reporting, and Record Keeping Order. The Order establishes specific procedures for banks with respect to customer identification, record keeping, and the reporting of irregular and suspicious transactions in keeping with the recommendations of the Basel Committee on Banking Supervision. The Supervisor of Banks at the Bank of Israel monitors compliance among banking institutions. Bankers and others are protected by law with respect to their cooperation with law enforcement entities.

Subsequent regulations established the methods of reporting to the Customs Authority (a part of the Israel Tax Authority) monies brought in or out of Israel, and criteria for financial sanctions for violating the law, as well as for appeals. The regulations require the declaration of currency transferred (including cash, travelers' checks, and banker checks) into or out of Israel for sums above 80,000 new Israeli shekels (NIS) (approximately U.S. $20,000). This applies to any person entering or leaving Israel, and to any person bringing or taking money into or out of Israel by mail or any other methods, including cash couriers. Failure to comply is punishable by up to six months imprisonment or a fine of NIS 202,000 (approximately $50,500), or ten times the amount that was not declared, whichever is higher. Alternatively, an administrative sanction of NIS 101,000 (approximately U.S. $25,250), or five times the amount that was not declared, may be imposed by the Committee for Imposition of Financial Sanctions. In 2003, the Government of Israel (GOI) lowered the threshold for reporting cash transaction reports (CTRs) to NIS 50,000 (approximately U.S. $12,250), lowered the document retention threshold to NIS 10,000 (approximately U.S. $2,500), and imposed more stringent reporting requirements.

Clarifications to the PMLL were approved in Orders 5761-2001 and 5762-2002 requiring that suspicious transactions be reported by members of the stock exchange, portfolio managers, insurers or insurance agents, provident funds and companies managing a provident fund, providers of currency services, and the Postal Bank. Portfolio managers and members of the stock exchange are supervised by the Chairman of the Israel Securities Authority; insurers and insurance agents are under the authority of the Superintendent of Insurance in the Ministry of Finance; provident funds and companies managed by a provident fund are overseen by the Commissioner of the Capital Market in the Ministry of Finance, and the Postal Bank is monitored by the Minister of Communications. The PMLL does not apply at this time to intermediaries, such as lawyers and accountants.

Other subsequent changes to the PMLL authorized: the issuance of regulations requiring financial service providers to identify, report, and keep records for specified transactions for seven years; the establishment of a mechanism for customs officials to input into the IMPA database; the creation of regulations stipulating the time and method of bank reporting; the creation of rules on safeguarding the IMPA database; and rules for requesting and transmitting information between IMPA, the INP and the Israel Security Agency (ISA, or Shin Bet). The PMLL also imposed an obligation on financial service providers to report any IMPA activities perceived as unusual.

Order 5762 added money services businesses (MSB) to the list of entities required to file cash transaction reports (CTRs) and suspicious transaction reports (STRs) by size and type, and required that they preserve transaction records for at least seven years. The PMLL mandates the registration of MSBs through the Providers of Currency Services Registrar at the Ministry of Finance. A person engaging in the provision of currency services without being registered is liable to one year of imprisonment or a fine of NIS 600,000 (U.S. $150,000). In 2004, Israeli courts convicted several MSBs for failure to register with the Registrar of Currency Services, and a number of indictments are still pending. The INP and the Financial Service Providers Regulatory Authority maintain a high level of coordination, routinely exchange information, and have conducted multiple joint enforcement actions.

On July 11, 2007 a draft bill for PMLL (Amendment No. 7) 5776-2007 was published for the purpose of extending Israel's AML regime to the trade in precious stones (including Israel's substantial diamond trading industry). The bill passed the first vote in the Knesset on August 16, and has been submitted to committee for review. The amendment defines "dealers in precious stones" as those merchants whose annual transactions reach NIS 50,000 (approximately U.S. $11,800). It places significant obligations on dealers to verify the identity of their clients, report all transactions above a designated threshold (and all unusual client activity) to IMPA, as well as to maintain all transaction records and client identification for at least five years. The Customs Authority continues to intercept unreported diamond shipments, despite the fact that Israel imposes no tariffs on diamond imports.

In October 2006, the Knesset Committee on Constitution, Law and Justice approved an amendment to the Banking Order and the Regulations on the Prohibition on Financing Terrorism. The Order and Regulations were additional steps in the legislation intended to combat the financing of terrorism while maintaining correspondent and other types of banking relationships between Israeli and Palestinian commercial banks. Although the amendment to the Order and the Regulations impose serious obligations on banks to examine clients and file transaction reports, banks are still exempted from criminal liability if, inter alia, they fulfill all of their obligations under the Order (though they are not protected from civil liability). The Banking Order was expanded to cover the prohibition on financing terrorism and includes obligations to check the identification of parties to a transaction against declared terrorists and terrorist organizations, as well as obligations to report by size and type of transaction. The Banking Order sets the minimum size of a transaction that must be reported at NIS 5,000 (approximately U.S. $1,180) for transactions with a high-risk country or territory. The order also includes examples for unusual financial activity suspected to be related to terrorism, such as transfers from countries with no anti-money laundering or counterterrorist finance (AML/CTF) regime to nonprofit organizations (NGOs) within Israel and the occupied territories.

In 2007, Israel took steps to implement Cabinet Decision 4618, passed on January 1, 2006, by creating an interagency "fusion center" and six interagency task forces for pursuing financial crimes. The regulation explicitly instructs the INP and the Shin Bet to target illicit proceeds as a primary objective in the war on organized crime. As Israel does not have legislation preventing financial service companies from disclosing client and ownership information to bank supervisors and law enforcement authorities, the new regulation establishes conditions for the use of such information to avoid its abuse and to set guidelines for the police and security services.

Israel has established systems for identifying, tracing, freezing, seizing, and forfeiting narcotics-related assets, as well as assets derived from or intended for other serious crimes, including the funding of terrorism and trafficking in persons. The law also allows for civil forfeiture when ordered by the District Court. The identification and tracing of such assets is part of the ongoing function of the Israeli intelligence authorities and IMPA. The INP has responsibility for seizing assets and the State Attorney's Office has authority to freeze assets. Banking institutions cooperate fully, and often freeze suspicious assets according to guidance from the INP and Ministry of Defense. Israel's International Legal Assistance Law enables Israel to offer full and effective cooperation to authorities in foreign states, including enforcement of foreign forfeiture orders in terror financing cases (both civil and criminal).

In December 2004, the Israeli Parliament adopted the prohibition on terrorist financing law 5765-2004, which is geared to further modernize and enhance Israel's ability to combat terrorist financing and to cooperate with other countries on such matters. The Law went into effect in August 2005, criminalizing the financing of terrorism as required by United Nations Security Council Resolution (UNSCR) 1373. The Israeli legislative regime criminalizing the financing of terrorism includes provisions of the Defense Regulations State of Emergency/1945, the Prevention of Terrorism Ordinance/1948, the Penal Law/1977, and the PMLL. Under the International Legal Assistance Law of 1998, Israeli courts are empowered to enforce forfeiture orders executed in foreign courts for crimes committed outside Israel.

In December 2007, the Knesset Law Committee approved new regulations enabling the declaration by a ministerial committee of foreign designated terrorists, and legally requiring financial institutions to comply with the foreign designations. The National Security Council legal counsel has responsibility for referring foreign designations to the committee for adoption under Israeli law, and is expected to include entities on the UNSCR 1267 Sanctions Committee consolidated list and entities on the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. Once designated, identifying information for the terrorist entity is to be published on the Ministry of Defense website, in two daily newspapers, the Official Gazette of the Israeli Government, and

distributed by email to financial institutions. Israel already enforces UNSCR 1267 under its Trade with the Enemy Ordinance of 1939, and regularly notifies financial institutions of restricted entities.

The ISA is responsible for investigating terrorist financing offenses, while the Israel Tax Authority handles investigations originating in customs offenses. Under Israeli law, it is a felony to conceal cash transfers upon entry to the West Bank or Gaza, and the agencies coordinate closely to track funds that enter Israeli ports. Customs and the Ministry of Defense also cooperate in combating trade-based terrorist financing, including goods destined for terrorist entities in the West Bank or Gaza.

The INP reports no indications of an overall increase in financial crime relative to previous years. In 2007, IMPA reported 56 arrests and five prosecutions relating to money laundering and/or terrorist financing. In 2007, IMPA received 10,597 suspicious transaction reports. During this period IMPA disseminated 552 intelligence reports to law enforcement agencies and to foreign FIUs in response to requests, and on its own initiative. In addition, eight different investigations yielded indictments (some of them multiple indictments) and ten resulted in convictions or plea bargains. In 2007, the INP seized approximately U.S. $9 million in suspected criminal assets, a decrease from U.S. $12 million in 2006 and U.S. $75 million seized in 2005.

Israel is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. In December 2006 Israel ratified the UN Convention against Transnational Organized Crime. The IMPA is a member of the Egmont Group, and Israel has been an active observer in MONEYVAL since 2006. Israel has signed but not yet ratified the UN Convention against Corruption. Israel is the only nonmember of the Council of Europe to become a party to the European Convention on Mutual Assistance in Criminal Matters (in 1967) and its Second Additional Protocol (in 2006), which is designed to provide more effective and modern means of assisting member states in law enforcement matters. There is a Mutual Legal Assistance Treaty in force between the United States and Israel, as well as a bilateral mutual assistance agreement in customs matters. Customs, IMPA, the INP and the Israel Securities Agencies routinely exchange information with U.S. agencies through their regional liaison offices, as well as through the Israel Police Liaison Office in Washington. In 2007, Israel provided unprecedented assistance in sharing evidence critical to the prosecution of terrorist financing cases in the United States, allowing for the first time the testimony of intelligence agents in U.S. courts.

The Government of Israel continued to make progress in strengthening its anti-money laundering and terrorist financing regime in 2007. Israel should continue the aggressive investigation of money laundering activity associated with organized criminal operations and syndicates. Israel should also continue its efforts to address the misuse of the international diamond trade to launder money by approving draft legislation. Under the new terrorist financing amendment, Israel should adopt appropriate foreign designations of terrorist entities in a timely manner.

## Italy

Italy is fully integrated in the European Union (EU) single market for financial services. Money laundering is a concern both because of the prevalence of homegrown organized crime groups and the recent influx of criminal organizations from abroad, especially from Albania, Romania, Russia, China, and Nigeria.

The heavy involvement in international narcotics trafficking of domestic and Italian-based foreign organized crime groups complicates counternarcotics activities. Italy is both a consumer country and a major transit point for heroin coming from the Near East and Southwest Asia through the Balkans en route to Western/Central Europe and, to a lesser extent, the United States. Italian and ethnic Albanian criminal organizations work together to funnel drugs to Italy and, in many cases, on to third countries.

Additional important trafficking groups include other Balkan organized crime entities, as well as Nigerian, Colombian, and other South American trafficking groups.

In addition to the narcotics trade, laundered money originates from a myriad of criminal activities, such as alien smuggling, pirated and counterfeited goods, extortion, and usury. Financial crimes not directly linked to money laundering, such as credit card and Internet fraud, are increasing. Italy is not an offshore financial center.

Money laundering occurs both in the regular banking sector and in the nonbank financial system, including casinos, money transfer houses, and the gold market. Money launderers predominantly use nonbank financial institutions for the illicit export of currency, primarily U.S. dollars and euros, to be laundered in offshore companies. There is a substantial black market for smuggled goods in the country, but it is not funded significantly by narcotics proceeds. According to Italy's Central Institute of Statistics (ISTAT), Italy's "underground" economic activity may be as large as 18 percent of the GDP. Much of this "underground activity is not related to organized crime, but is instead part of efforts to avoid taxation."

According to a 2006 International Monetary Fund evaluation, Italy's anti-money laundering and counter-terrorist financing system is comprehensive. Money laundering is defined as a criminal offense when laundering relates to a separate, intentional felony offense. All intentional criminal offenses are predicates to the crime of money laundering, regardless of the applicable sentence for the predicate offense. With approximately 600 money laundering convictions a year, Italy has one of the highest rates of successful prosecutions in the world.

Italy has strict laws on the control of currency deposits in banks. In June of 2007, the Ministry of Finance issued a decree bringing Italy into compliance with EU regulation 1889/2005 on controls of cash entering or leaving the European Community. Banks must identify their customers and record any transaction that exceeds 5000 euros (approximately U.S. $7,300). The previous threshold was 12,500 euros (approximately U.S. $18,250). Bank of Italy mandatory guidelines require the reporting of all suspicious cash transactions and other activity, such as a third party payment on an international transaction. Italian law prohibits the use of cash or negotiable bearer instruments for transferring money in amounts in excess of 5,000 euros (approximately U.S. $7,300), except through authorized intermediaries or brokers.

Banks and other financial institutions are required to maintain for ten years records necessary to reconstruct significant transactions, including information about the point of origin of funds transfers and related messages sent to or from Italy. Banks operating in Italy must record account data on their own standardized customer databases established within the framework of the anti-money laundering regulation. A "banker negligence" law makes individual bankers responsible if their institutions launder money. The law protects bankers and others with respect to their cooperation with law enforcement entities.

Italy has addressed the problem of international transportation of illegal-source currency and monetary instruments by applying the 10,000 euros (U.S. $14,700) equivalent reporting requirement to cross-border transport of domestic and foreign currencies and negotiable bearer instruments. Reporting is mandatory for cross-border transactions involving negotiable bearer monetary instruments. Financial institutions are required to maintain a uniform anti-money laundering database for all transactions (including wire transfers) over 5,000 euros ($7,300) and to submit this data monthly to the Italian Foreign Exchange Office (Ufficio Italiano dei Cambi, or UIC). The data is aggregated by class of transaction, and any reference to customers is removed. The UIC analyzes the data and can request specific transaction details if warranted. In 2008, this operation will be handled by the newly created Financial Intelligence Unit.

In 2005, the UIC received 8,576 suspicious transaction reports (STRs) related to money laundering and 482 related to terrorist financing. Italian law requires that the Anti-Mafia Investigative Unit (DIA) and the Guardia di Finanza (GdF) be informed about almost all STRs, including those that the UIC does not pursue further. The UIC does, however, have the authority to perform a degree of filtering before passing STRs to law enforcement. Law enforcement opened 328 investigations based on STRs, which resulted in 103 prosecutions.

Because of Italy's banking controls, narcotics traffickers are using different ways of laundering drug proceeds. To deter nontraditional money laundering, the Government of Italy (GOI) has enacted a decree to broaden the category of institutions and professionals subject to anti-money laundering regulations. The list now includes accountants, debt collectors, exchange houses, insurance companies, casinos, real estate agents, brokerage firms, gold and valuables dealers and importers, auction houses, art galleries, antiques dealers, labor advisors, lawyers, and notaries. The required implementing regulations for the decree, as far as nonfinancial businesses and professions are concerned, were issued in February 2006 and came into force in April 2006 (Ministerial Decrees no. 141, 142 and 143 of 3.02.2006). However, while Italy now has comprehensive internal auditing and training requirements for its (broadly-defined) financial sector, implementation of these measures by nonbank financial institutions lags behind that of banks, as evidenced by the relatively low number of STRs filed by nonbank financial institutions. As of 2005, according to UIC data, banking institutions submit about 80 percent of all STRs. Money remittance operators submit 13.5 percent of the total number of STRs, and all other sectors together account for less than ten percent.

Until January 1, 2008, the UIC served as Italy's financial intelligence unit (FIU). An arm of the Bank of Italy (BoI), the UIC received and analyzed STRs filed by covered institutions, and then forwarded them to either the Anti-Mafia Investigative Unit (DIA) or the Guardia di Finanza (GdF) (financial police) for further investigation. The UIC compiles a register of financial and nonfinancial intermediaries that carry on activities that could be exposed to money laundering. The UIC has access to banks' customer databases. Investigators from the GdF and other Italian law enforcement agencies must obtain a court order prior to being granted access to the archive. The UIC also performed supervisory and regulatory functions such as issuing decrees, regulations, and circulars. It does not require a court order to compel supervised institutions to provide details on regulated transactions. A special currency branch of the GdF is the Italian law enforcement agency with primary jurisdiction for conducting financial investigations in Italy. On January 1, 2008 Italy opened a Financial Intelligence Unit at the Bank of Italy that will assume the responsibilities of the UIC.

Italy has established reliable systems for identifying, tracing, freezing, seizing, and forfeiting assets from narcotics trafficking and other serious crimes, including terrorism. These assets include currency accounts, real estate, vehicles, vessels, drugs, legitimate businesses used to launder drug money, and other instruments of crime. Under anti-Mafia legislation, seized financial and nonfinancial assets of organized crime groups can be forfeited. The law allows for forfeiture in both civil and criminal cases. Through October 2004, Italian law enforcement seized more than 160 million euros (approximately $U.S. 233 million) in forfeited assets due to money laundering.

Italy does not have any significant legal loopholes that allow traffickers and other criminals to shield assets. However, the burden of proof is on the Italian government to make a case in court that assets are related to narcotics trafficking or other serious crimes. Law enforcement officials have adequate powers and resources to trace and seize assets; however, their efforts can be affected by which local magistrate is working a particular case. Funds from asset forfeitures are entered into the general State accounts. Italy shares assets with member states of the Council of Europe and is involved in negotiations within the EU to enhance asset tracing and seizure.

In October 2001, Italy passed a law decree (subsequently converted into law) that created the Financial Security Committee (FSC), charged with coordinating GOI efforts to track and interdict terrorist

financing. FSC members include the Ministries of Finance, Foreign Affairs, Home Affairs, and Justice; the BoI; UIC; CONSOB (Italy's securities market regulator); GdF; the Carabinieri; the National Anti-Mafia Directorate (DNA); and the DIA. The Committee has far-reaching powers that include waiving provisions of the Official Secrecy Act to obtain information from all government ministries.

A second October 2001 law decree (also converted into law) made financing of terrorist activity a criminal offense, with prison terms of between seven and fifteen years. The legislation also requires financial institutions to report suspicious activity related to terrorist financing. Both measures facilitate the freezing of terrorist assets. Per FSC data as of December 2004, 57 accounts had been frozen belonging to 55 persons, totaling U.S. $528,000 under United Nations (UN) resolutions relating to terrorist financing. Data for 2005 through 2007 has not been reported. The GOI cooperates fully with efforts by the United States to trace and seize assets. Italy is second in the EU only to the United Kingdom in the number of individual terrorists and terrorist organizations the country has submitted to the UN 1267 Sanctions Committee for designation.

The UIC disseminates to financial institutions the EU, UN, and U.S. Government lists of terrorist groups and individuals. The UIC may provisionally suspend for 48 hours transactions suspected of involving money laundering or terrorist financing. The courts must then act to freeze or seize the assets. Under Italian law, financial and economic assets linked to terrorists can be directly frozen by the financial intermediary holding them, should the owner be listed under EU regulation. Moreover, assets can be seized through a criminal sequestration order. Courts may issue such orders when authorities are investigating crimes linked to international terrorism or by applying administrative seizure measures originally conceived to fight the Mafia. The sequestration order may be issued with respect to any asset, resource, or item of property, provided that these are goods or resources linked to the criminal activities under investigation.

Law no. 15 of January 29, 2006, gave the government authority to implement the EU's Third Money Laundering Directive (Directive 2005/60/EC) and to issue provisions to make more effective the freezing of nonfinancial assets belonging to listed terrorist groups and individuals. Legislative Decree 231 of November 21, 2007 implements elements of the Third Money Laundering Directive.

In Italy, the term "alternative remittance system" refers to regulated nonbank institutions such as money transfer businesses. Informal remittance systems do exist, primarily to serve Italy's significant immigrant communities, and in some cases are used by Italy-based drug trafficking organizations to transfer narcotics proceeds.

Italy does not regulate charities as such. Primarily for tax purposes, in 1997 Italy created a category of "not-for-profit organizations of social utility" (ONLUS). Such organizations can be associations, foundations or fundraising committees. To be classified as an ONLUS, the organization must register with the Finance Ministry and prepare an annual report. There are currently 19,000 registered entities in the ONLUS category. Established in 2000, the ONLUS Agency issues guidelines and drafts legislation for the nonprofit sector, alerts other authorities of violations of existing obligations, and confirms de-listings from the ONLUS registry. The ONLUS Agency cooperates with the Finance Ministry in reviewing the conditions for being an ONLUS. The ONLUS Agency has reviewed 1,500 entities and recommended the dissolution of several that were not in compliance with Italian law. Italian authorities believe that there is a low risk of terrorist financing in the Italian nonprofit sector.

Italian cooperation with the United States on money laundering has been exemplary. The United States and Italy have signed a customs mutual assistance agreement, as well as extradition and mutual legal assistance treaties. Both in response to requests under the mutual legal assistance treaty (MLAT) and on an informal basis, Italy provides the United States records related to narcotics-trafficking, terrorism and terrorist financing investigations and proceedings. Italy also cooperates closely with U.S. law enforcement agencies and other governments investigating illicit financing related to these

and other serious crimes. Currently, assets can only be shared bilaterally if agreement is reached on a case-specific basis. In May 2006, however, the U.S. and Italy signed a new bilateral instrument on mutual legal assistance as part of the process of implementing the U.S./EU Agreement on Mutual Legal Assistance, signed in June 2003. Once ratified, the new U.S./Italy bilateral instrument on mutual legal assistance will provide for asset forfeiture and sharing.

Italy 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 Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. Italy has also signed, but has not yet ratified, the UN Convention against Corruption.

Italy is an active member of the Financial Action Task Force (FATF). Italy co-chaired FATF's International Cooperation Working Group in 2007. Italy's FIU, the UIC, is a member of the Egmont Group. The UIC has been authorized to conclude information-sharing agreements concerning suspicious financial transactions with other countries. To date, the FIU has signed memoranda of understanding with 12 analogs, primarily in Europe and is negotiating agreements with 8 other FIUs, primarily in Asia. Italy has a number of bilateral agreements with foreign governments in the areas of investigative cooperation on narcotics trafficking and organized crime. Reportedly, there is no known instance of refusal to cooperate with foreign governments.

The Government of Italy is firmly committed to the fight against money laundering and terrorist financing, both domestically and internationally. However, given the relatively low number of STRs being filed by nonbank financial institutions, the GOI should improve its training efforts and supervision in this sector. Italian law enforcement agencies should take additional steps to understand and identify underground finance and value transfer methodologies employed by Italy's burgeoning immigrant communities. The GOI should also continue its active participation in multilateral efforts dedicated to the global fight against money laundering and terrorist financing.

## Jamaica

Jamaica, the foremost producer and exporter of marijuana in the Caribbean, is also a major transit country for cocaine flowing from South America to the United States and other international destinations. In addition to profits from domestic marijuana trafficking, payments for cocaine and weapons pass through Jamaica in the form of bulk cash shipments back to South America. These illegal drug flows must be legitimated and therefore make Jamaica susceptible to money laundering activities and other financial crimes. In 2007, there was not a significant increase in the occurrence of financial crimes; however, there was a noticeable upsurge in advance fee scams and other related fraud schemes, including unregulated "investment clubs." The Government of Jamaica (GOJ) is also becoming increasingly concerned by the high rate of trade-based money laundering and has plans to attack this problem in 2008.

Jamaica is neither an offshore financial center, nor is it a major money laundering country. Currently, Jamaican banking authorities do not license offshore banks or other forms of exempt or shell companies, nor are nominee or anonymous directors and trustees allowed for companies registered in Jamaica. Financial institutions are prohibited from maintaining anonymous, numbered or fictitious accounts under the 2007 Proceeds of Crime Act. As part of its political campaign, the new government, which took office in September, promoted the idea of turning Kingston into an offshore financial center. If this plan were to come to fruition, it could increase Jamaica's vulnerability to money laundering. The GOJ does not encourage or facilitate money laundering, nor has any senior official been investigated or charged with the laundering of proceeds from illegal activity. Public corruption, particularly in the Customs Service, provides opportunities for trade-based money laundering. The majority of funds being laundered in Jamaica are from drug traffickers and elements

of organized crime, mainly the profits obtained in their overseas criminal activities. There is no evidence of terrorist financing in Jamaica.

Due to scrutiny by banking regulators, Jamaican financial instruments are considered an unattractive mechanism for laundering money. As a result, much of the proceeds from drug trafficking and other criminal activity are used to acquire tangible assets such as real estate or luxury cars, as well as legitimate businesses. Over the last year a significant amount of assets have flowed into new, unregulated financial investment clubs and loan schemes, which are ripe for exploitation by criminal elements. There is a significant black market for smuggled goods, which is due to tax evasion. Further complicating the ability of the GOJ to track and prevent money laundering and the transit of illegal currency through Jamaica are the hundreds of millions of U.S. dollars in remittances sent home by the substantial Jamaican population overseas.

There is a free trade zone in Montego Bay, which has a small cluster of information technology companies, and one gaming entity that focuses on international gambling. There is no indication that this free zone is being used for trade-based money laundering or terrorist financing. Domestic casino gambling, Para mutual wagering and lotteries are permitted in Jamaica, and are regulated by the Betting Gaming and Lotteries Commission.

The Proceeds of Crime Act (POCA), which became effective in May 2007, incorporates the existing provisions of its predecessor legislation (the Money Laundering Act and the Drug Offences Forfeiture of Proceeds Act), and now allows for both civil and criminal forfeiture of assets related to criminal activity. The POCA criminalizes money laundering related to narcotics offenses, fraud, firearms trafficking, human trafficking, terrorist financing and corruption, and applies to all property or assets associated with an individual convicted or suspected of involvement with a crime. This includes legitimate businesses used to launder drug money or support terrorist activity. Bank secrecy laws exist; however, there are provisions under GOJ law to enable law enforcement access to banking information.

The POCA establishes a five-year record-keeping requirement for both transactions and client identification records, and requires financial institutions to report all currency transactions over U.S. $15,000. Money transfer or remittance companies have a reporting threshold of U.S. $5,000, while for exchange bureaus the threshold is U.S. $8,000. The POCA requires banks, credit unions, merchant banks, wire-transfer companies, exchange bureaus, mortgage companies, insurance companies, brokers and other intermediaries, securities dealers, and investment advisors to report suspicious transactions of any amount to Jamaica's financial intelligence unit (FIU), which is a unit within the Ministry of Finance's Financial Investigations Division (FID). Based on its analysis of cash threshold reports and suspicious transaction reports (STRs), the FIU forwards cases to the Financial Crimes Unit of the FID for further investigation. There is also a Financial Crimes Division established within the Jamaica Constabulary Force, and it is unclear how its investigative responsibilities for financial crimes are shared with the Financial Crimes Unit of the FID.

Jamaica's central bank, the Bank of Jamaica, supervises the financial sector for compliance with anti-money laundering and counter-terrorist financing provisions. Although the POCA permits the Minister of Finance to add nonbanking institutions to the list of obligated reporting entities, a court decision that has been pending for months has thus far tied the government's hands with respect to a growing number of currently unregulated "investment clubs, some of which are suspected to serve as covers for Ponzi schemes.

The FID was originally created by a merger, within the Ministry of Finance, the Revenue Protection Department, and the Financial Crimes Unit. The merger resulted in a division with seven distinct units. The FID currently consists of 14 forensic examiners, six police officers who have full arrest powers, a director and five administrative staff. The FID is working with the United Kingdom and Ireland to develop a comprehensive, in-house capacity for training the additional staff members it was authorized

to meet its additional duties under POCA. The FID currently needs additional lawyers, forensic accountants, police officers and intelligence analysts. In the past, FID staff enjoyed a salary premium that made the positions more attractive. Recent changes have raised civil service salaries in line with current salary levels at the FID, and without revision to its pay scale, the FID's ability to recruit qualified and motivated staff will remain limited.

The FID has access to data from other government sources, which include the national vehicle registry, property tax rolls, duty and transfer rolls, various tax databases, national land register, and cross border currency declarations. Direct information access to these databases is limited to a small number of people within the FID. Indirect access is available through an internal mechanism that funnels requests to authorized users. Companion legislation to the POCA, the FID Act, which was supposed to have been enacted in 2007, remains stalled. The FID Act would bring Jamaica's regulations fully in line with the international standards of the Egmont Group, and allow for information exchange between the FID and other FIUs.

In mid-2007, the FID and the Tax Administrative Directorate (TAAD) signed a protocol for cooperation on investigations that have a nexus to criminal tax evasion. Because both entities suffer from a lack of adequate resources, it remains to be seen if the protocol can overcome competing priorities (such as revenue collection obligations, a main focus of the GOJ) and permit TAAD staff to assist the FID with money laundering investigations.

Jamaica has an ongoing education program to ensure compliance with the mandatory suspicious transaction reporting requirements. Reporting individuals are protected by law with respect to their cooperation with law enforcement entities. The FID reports that nonbank financial institutions have a 70 percent compliance rate with money laundering controls. There are currently no statistics available on the numbers of STRs, cases and convictions for 2007.

The Jamaican Parliament's 2004 amendments to the Bank of Jamaica Act, the Banking Act, the Financial Institutions Act, and the Building Societies Act improve the governance, examination and supervision of commercial banks and other financial institutions by the Bank of Jamaica. Amendments to the Financial Services Commission Act, which governs financial entities supervised by the Financial Services Commission, expand the powers of the authorities to share information, particularly with overseas regulators and law enforcement agencies. The amended Acts provide the legal and policy parameters for the licensing and supervision of financial institutions, and lay a complementary foundation to the POCA. Guidelines issued by the Bank of Jamaica caution financial institutions against initiating or maintaining relationships with persons or businesses that do not meet the standards of the Financial Action Task Force.

The GOJ requires customs declaration of currency or monetary instruments over U.S. $10,000 or its equivalent. The Kingston-based Airport Interdiction Task Force, a joint law enforcement effort by the United States, United Kingdom, Canada and Jamaica, began operations in mid-2007. The Task Force focuses, in part, on efforts to combat the movement of large amounts of cash often in shipments totaling hundreds of thousands of U.S. dollars through Jamaica.

The POCA expands the confiscation powers of the GOJ and permits, upon conviction, the forfeiture of assets assessed to have been received by the convicted party within the six years preceding the conviction. Under the POCA, the Office of the Public Prosecutor and the FID have the authority to bring asset freezing and forfeiture orders before the court. However, both agencies are lacking in staff and resources, and few of the prosecutors have received substantive training on financial crimes.

Under the POCA, the proposed division of forfeited assets would distribute assets equally among the Ministry of National Security, the Ministry of Finance, and the Ministry of Justice. An Assets Recovery Agency (ARA) will be established within the FID to manage seized and forfeited assets. There is currently no data available on the amount of seizures and forfeitures of assets for 2007. In

2006, U.S. $2 million was seized and U.S. $1.5 million was forfeited. Nondrug related assets go to a consolidated or general fund, while drug related assets are placed into a forfeited asset fund, which benefits law enforcement.

The Terrorism Prevention Act of 2005 criminalizes the financing of terrorism, consistent with UN Security Council Resolution 1373. Under the Terrorism Prevention Act, the GOJ has the authority to identify, freeze, and seize terrorist finance-related assets. The FID has the responsibility for investigating terrorist financing. The FID is currently updating its FIU database and will be implementing a system to cross-reference reports from the U.S. Treasury Department's Office of Foreign Asset Control (OFAC) and the UN Sanctions Committee. Additionally, the Ministry of Foreign Affairs and Foreign Trade circulates to all relevant agencies the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee consolidated list. To date, no accounts owned by those included on the UN consolidated list have been identified in Jamaica, nor has the GOJ encountered any misuse of charitable or nonprofit entities as conduits for the financing of terrorism.

Jamaica and the United States have a Mutual Legal Assistance Treaty that entered into force in 1995, as well as an agreement for the sharing of forfeited assets, which became effective in 2001. Jamaica is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the Inter-American Convention against Corruption, and the UN Convention against Transnational Organized Crime. The GOJ has signed, but not ratified, the UN Convention against Corruption. Jamaica is a member of the Caribbean Financial Action Task Force (CFATF) and the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Until the FID Act is passed, the FID will not meet the membership requirements of the Egmont Group.

The Government of Jamaica has moved forward in its efforts to combat money laundering and terrorist financing with the passage of the Proceeds of Crime Act, and should now ensure that the Act is fully implemented. The GOJ should resolve whether the POCA and other financial regulations apply to "investment clubs" and other alternative schemes. The GOJ should ensure the swift passage of the FID Act to qualify the FIU within the Financial Investigations Division to meet the international standards of the Egmont Group and exchange information with other FIUs. In addition, the GOJ should grant the FID adequate resources to enable it to hire an appropriate number of staff to allow for the additional work it now faces with the implementation of the POCA. The GOJ should also ensure that a duality of functions does not exist in the investigative responsibilities of the Financial Crimes Unit of the FID and the Financial Crimes Division of the Jamaican Constabulary Force. The GOJ should also ratify the UN Convention against Corruption.

## Japan

Japan is the world's second largest economy and an important world financial center. Although the Japanese government continues to strengthen legal institutions to permit more effective enforcement of financial transaction laws, Japan still faces substantial risk of money laundering by organized crime and other domestic and international criminal elements. The principal sources of laundered funds are drug trafficking and financial crimes: illicit gambling, loan-sharking, extortion, abuse of legitimate corporate activities, Internet fraud activities, and all types of property related crimes, which are often linked to Japan's criminal organizations. U.S. law enforcement investigations periodically show a link between drug-related money laundering activities in the U.S. and bank accounts in Japan.

On March 29, 2007, Japan's government enacted new money laundering "Law for Prevention of Transfer of Criminal Proceeds." Referred to in the press as the Gatekeeper Bill, after the Financial Action Task Force (FATF) Gatekeeper Initiative, and designed to bring Japan into closer compliance with the FATF Forty Recommendations, the bill's passage marked significant changes in Japan's anti-

money laundering landscape. In addition to the financial institutions previously regulated, the new statutes expanded the types of nonfinancial businesses and professions under the law's purview, including real estate agents, private mail box agencies, dealers of precious metals and stones; and, certain types of trust and company service providers. They must conduct customer due diligence, confirm client identity, retain customer verification records, and report Suspicious Transaction Reports (STRs) to the authorities. Legal and accounting professionals such as judicial scriveners and certified public accounts are now subject to customer due diligence and record keeping, but not STR reporting. However, the bill stipulates that, "confirmation of the identity of the clients and retention of records (of transaction and identity verification) by lawyers shall be prescribed by the Japan Federation Bar Association's regulation," permitting lawyers to remain outside the law's new parameters. Accordingly, the bar association drafted and now enforces "Rules Regarding the Verification of Clients' Identity and Record-Keeping."

Drug-related money laundering was first criminalized under the Anti-Drug Special Law that took effect July 1992. This law also mandates the filing of STRs for suspected proceeds of drug offenses, and authorizes controlled drug deliveries. The legislation also creates a system to confiscate illegal profits gained through drug crimes. The seizure provisions apply to tangible and intangible assets, direct illegal profit, substitute assets, and criminally derived property that have been commingled with legitimate assets.

The narrow scope of the Anti-Drug Special Law and the burden required of law enforcement to prove a direct link between money and assets to specific drug activity limits the law's effectiveness. As a result, Japanese police and prosecutors have undertaken few investigations and prosecutions of suspected money laundering. Many Japanese officials in the law enforcement community, including Japanese Customs, believe that Japan's organized crime groups have been taking advantage of this limitation to launder money.

Japan expanded its money laundering law beyond narcotics trafficking to include money laundering predicate offenses such as murder, aggravated assault, extortion, theft, fraud, and kidnapping when it passed the 1999 Anti-Organized Crime Law (AOCL), which took effect in February 2000. The law extends the confiscation laws to include additional money laundering predicate offenses and value-based forfeitures, and enhances the suspicious transaction reporting system.

The AOCL was partially revised in June of 2002 by the "Act on Punishment of Financing to Offenses of Public Intimidation," which specifically added the financing of terrorism to the list of money laundering predicates. A further amendment to the AOCL submitted to the Diet for approval in 2004, designed to expand the predicate offenses for money laundering from approximately 200 offenses to nearly 350 offenses, with almost all offenses punishable by imprisonment, has yet to be approved.

Japan's Financial Services Agency (FSA) supervises all financial institutions and the Securities and Exchange Surveillance Commission supervises securities transactions. The FSA classifies and analyzes information on suspicious transactions reported by financial institutions, and provides law enforcement authorities with information relevant to their investigation. Japanese banks and financial institutions are required by law to record and report the identity of customers engaged in large currency transactions. There are no secrecy laws that prevent disclosure of client and ownership information to bank supervisors and law enforcement authorities.

To facilitate the exchange of information related to suspected money laundering activity, the FSA established the Japan Financial Intelligence Office (JAFIO) on February 1, 2000, as Japan's financial intelligence unit. Under the 2007 anti-money laundering law, on April 1, 2007, JAFIO relocated from the FSA to the National Police Agency, where it is known as the Japan Financial Intelligence Center (JAFIC). Correspondingly, JAFIC's staff grew from 17 to 43 personnel, with an emphasis on strengthened analytical functions. JAFIC receives STRs from specified business operators through the

competent administrative authorities, analyzes them, and disseminates intelligence deemed useful to criminal investigations to the law enforcement community.

In 2006, JAFIC received 113,860 STRs, up from the 98,935 STRs received in 2005. In 2006, some 82 percent of the reports were submitted by banks, 7 percent by credit cooperatives, 9 percent from the country's large postal savings system, 0.7 percent from nonbank money lenders, and almost none from insurance companies. In 2006, JAFIC disseminated 71,241 STRs to law enforcement, up from 66,812 STRs disseminated in 2005. Of these, 143 money laundering cases went to prosecutors, up from 112 in 2005. The amount of money confiscated or forfeited in 2006 was 6.07 billion yen (U.S. $52 million), up from 4.46 billion yen (U.S. $39 million) in 2005.

As of 2007, JAFIC has concluded international cooperation agreements with numerous counterpart FIU's (Australia, Belgium, Brazil, Canada, Hong Kong, Indonesia, Malaysia, the Philippines, Singapore, Thailand, the United Kingdom, and the United States). These agreements establish cooperative frameworks for the exchange of financial intelligence related to money laundering and terrorist financing. Japanese financial institutions have cooperated with law enforcement agencies, including U.S. and other foreign government agencies investigating financial crimes related to narcotics.

In 2006, Japan concluded a Mutual Legal Assistance Treaty (MLAT) with the Republic of Korea, and is currently negotiating MLAT texts with China and Russia. In 2003, the United States and Japan concluded a Mutual Legal Assistance Treaty (MLAT), which took effect in July of 2006. In 2007 the U.S.-Japan MLAT was used for the first time in furtherance of two separate money laundering investigations where the predicate crimes (Nigerian bank fraud) first occurred overseas, then moved to the U.S., with the money subsequently laundered in Japan; the cases are still pending.

Although Japan has not adopted "due diligence" or "banker negligence" laws to make individual bankers legally responsible if their institutions launder money, there are administrative guidelines that require due diligence. In a high-profile 2006 court case, however, the Tokyo District Court ruled to acquit a Credit Suisse banker of knowingly assisting an organized crime group to launder money despite doubts about whether the banker performed proper customer due diligence. Japanese law does not protect bankers and other financial institution employees who cooperate with law enforcement entities.

In April 2002, the Diet enacted the Law on Customer Identification and Retention of Records on Transactions with Customers by Financial Institutions (a "know your customer" law). The law reinforced and codified the customer identification and record-keeping procedures that banks had practiced for years. The Foreign Exchange and Foreign Trade law was revised in January 2007, so that financial institutions are required to make positive customer identification for both domestic transactions and transfers abroad in amounts of more than 100,000 yen (approximately $900). Banks and financial institutions are required to maintain customer identification records for seven years. In January 2007, an amendment to the rule on Customer Identification by Financial Institutions came into force, whereby financial institutions are now required to identify the originators of wire transfers of over 100,000 yen.

In 2004, the FSA cited Citibank Japan's failure to properly screen clients under anti-money laundering mandates as one of a list of problems that caused the FSA to shut down Citibank Japan's private banking unit. In February 2004, the FSA disciplined Standard Chartered Bank for failing to properly check customer identities and for violating the obligation to report suspicious transactions. In January 2007, the Federal Reserve ordered Japan's Sumitomo Mitsui Banking Corp.'s New York branch to address anti-money laundering deficiencies, only a month after similarly citing Bank of Tokyo-Mitsubishi UFJ for anti-money laundering shortcomings.

The Foreign Exchange and Foreign Trade Law requires travelers entering and departing Japan to report physically transported currency and monetary instruments (including securities and gold weighing over one kilogram) exceeding one million yen (approximately U.S. $8,475), or its equivalent in foreign currency, to customs authorities. Failure to submit a report, or submitting a false or fraudulent one, can result in a fine of up to 200,000 yen (approximately $1,695) or six months' imprisonment. Efforts by authorities to counter bulk cash smuggling in Japan are not yet matched by a commensurate commitment in necessary resources.

In response to the events of September 11, 2001 the FSA used the anti-money laundering framework provided in the Anti-Organized Crime Law to require financial institutions to report transactions where funds appeared either to stem from criminal proceeds or to be linked to individuals and/or entities suspected to have relations with terrorist activities. The 2002 Act on Punishment of Financing of Offenses of Public Intimidation, enacted in July 2002, added terrorist financing to the list of predicate offenses for money laundering, and provided for the freezing of terrorism-related assets. Japan signed the UN International Convention for the Suppression of the Financing of Terrorism on October 30, 2001, and became a party on June 11, 2002.

After September 11, 2001, Japan has regularly searched for and designated for asset freeze any accounts that might be linked to all the suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and the list of individuals and entities under UNSCR 1373.

Underground banking systems operate widely in Japan, especially in immigrant communities. Such systems violate the Banking Law. There have been a large number of investigations into underground banking networks. Reportedly, substantial illicit proceeds have been transferred abroad, particularly to China, North and South Korea, and Peru. In November 2004, the Diet approved legislation banning the sale of bank accounts, in a bid to prevent the use of purchased accounts for fraud or money laundering.

Japan has not enacted laws that allow for sharing of seized narcotics assets with other countries. However, the Japanese government fully cooperates with efforts by the United States and other countries to trace and seize assets, and makes use of tips on the flow of drug-derived assets from foreign law enforcement efforts to trace funds and seize bank accounts.

Japan is a party to the 1988 UN Drug Convention and has signed but not ratified the UN Transnational Organized Crime Convention. Ratification of this convention would require amendments to Japan's criminal code to permit charges of conspiracy, which is not currently an offense. Minority political parties and Japan's law society have blocked this amendment on at least three occasions. Japan is a member of the Financial Action Task Force. JAFIO (now JAFIC) joined the Egmont Group of FIUs in 2000. Japan is also a member of the Asia/Pacific Group against Money Laundering, and is scheduled for a second round mutual evaluation in 2008.

In 2002, Japan's FSA and the U.S. Securities and Exchange Commission and Commodity Futures Trading Commission signed a nonbinding Statement of Intent (SOI) concerning cooperation and the exchange of information related to securities law violations. In January 2006 the FSA and the U.S. SEC and CFTC signed an amendment to their SOI to include financial derivatives. Japan is a signatory but not a party to the UN Convention against Corruption. Japan is listed 17 out of 179 countries surveyed in Transparency International's 2007 Corruption Perception Index.

The Government of Japan has many legal tools and agencies in place to successfully detect, investigate, and combat money laundering. However, there have been few successful money laundering prosecutions and convictions. To strengthen its money laundering regime, Japan should stringently enforce the Anti-Organized Crime Law, and amend the law with regard to charges of conspiracy. The narrow scope of the Anti-Drug Special Law has limited the law's effectiveness. Japan

should also enact penalties for noncompliance with the customer identification provisions of the Foreign Exchange and Trade Law, adopt measures to share seized assets with foreign governments, and enact banker "due diligence" provisions. Japan should continue to combat underground financial networks. Since Japan is a major trading power and the misuse of trade is often the facilitator in alternative remittance systems and value transfer schemes, Japan should take steps to identify and combat trade-based money laundering. Japan should also become a party to the UN Transnational Organized Crime Convention and the UN Convention against Corruption.

## Jersey

The Bailiwick of Jersey (BOJ), one of the Channel Islands, is an international financial center offering a sophisticated array of offshore services. A Crown Dependency of the United Kingdom, it relies on the United Kingdom for its defense and international relations. Due to Jersey's investment services, most of the illicit money in Jersey is derived from foreign criminal activity. Domestically, local drug trafficking and corruption of politically exposed persons (PEPs) are sources of illicit proceeds found in the country. Money laundering mostly occurs within Jersey's banking system, investment companies, and local trust companies.

The financial services industry consists of 48 banks; 1,086 funds; 953 trust companies (2005 statistic), and 175 insurance companies (2006 statistic), which are largely captive insurance companies. The menu of services includes investment advice, dealing management companies, and mutual fund companies. In addition to financial services, companies offer corporate services, such as special purpose vehicles for debt restructuring and employee share ownership schemes. For high net worth individuals, there are wealth management services. All regulated entities can sell their services to both residents and nonresidents. All financial businesses must have a presence in Jersey, and management must also be in Jersey. However, although Jersey does not provide offshore licenses, it administers a number of companies registered in other jurisdictions. These companies, known as "exempt companies," do not pay Jersey income tax and their services are only available to nonresidents.

The Jersey Finance and Economics Committee is the government body responsible for administering the law, regulating, supervising, promoting, and developing the Island's finance industry. The financial Services Commission (FSC) is the financial services regulator. In 2003, the International Monetary Fund (IMF) assessed Jersey's anti-money laundering (AML) regime. The IMF reported that it found the FSC to be in compliance with international standards. The IMF has scheduled a review and assessment of Jersey's financial frameworks for October 2008.

Jersey's main AML laws are the Drug Trafficking Offenses (Jersey) Law of 1988, which criminalizes money laundering related to narcotics trafficking, and the Proceeds of Crime (Jersey) Law, 1999, which extends the predicate offenses for money laundering to all offenses punishable by at least one year in prison. The FSC has recently formed a dedicated AML Unit to lead the Island's operational AML and counter-terrorist financing (CTF) strategy. The AML Unit will devise and implement a registration scheme for currently unregulated nonfinancial services businesses and professions entering an oversight regime for the first time. Under amendments being made to the Proceeds of Crime (Jersey) Law 1999, businesses such as estate agents and dealers in high value goods will, for the first time, have AML regulation. The AML Unit has also taken specific responsibility regulating money service business such as bureaux de change, check cashers, and money transmitters.

In May and July 2007, in preparation for the upcoming IMF assessment and with Council of Ministers approval, the AML/CTF Strategy Group issued three consultation papers proposing to extend and update Jersey's AML framework to comply with the international standards. In October 2007, the FSC published a Consultation Paper proposing amendments to current legislation and introducing new secondary legislation. The Consultation Paper discusses the proposed legislative changes with regard to the Trust Company Business and Investment Business secondary legislation on accounts, audits,

and reports. The paper also discusses requirements on Trust Company Business with respect to the safekeeping of customer money.

Financial institutions must report suspicious transactions under the narcotics trafficking, terrorism, and anti-money laundering laws. There is no threshold for filing a suspicious transaction report (STR), and the reporting individual is protected from criminal and civil charges by safe harbor provisions in the law. Banks and other financial service companies must maintain financial records of their customers for a minimum of 10 years after completion of business. The FSC has issued AML Guidance Notes that the courts take into account when considering whether or not an offense has been committed under the Money Laundering Order. Upon conviction of money laundering, a person could receive imprisonment of one year or more.

After consultation with the financial services industry, the FSC issued a position paper (jointly with Guernsey and Isle of Man counterparts) proposing to further tighten the essential due diligence requirements that financial institutions must meet regarding their customers. The position paper states the FSC's intention to insist on the responsibility of all financial institutions to verify the identity of their customers, regardless of the action of intermediaries. The paper also states an intention to require a progressive program to obtain verification documentation for customer relationships established before the Proceeds of Crime (Jersey) Law came into force in 1999. Each year working groups review specific portions of these principles and draft AML Guidance Notes to incorporate changes.

Following the extensive consultation with the Funds Sector, and approval by the State of Jersey in November 2007, the FSC published Codes of Practice for Fund Services Business. The Code consists of seven high level principles for the conduct of fund services business, together with more detailed requirements in relation to each principle.

Approximately 30,000 Jersey companies have registered with the Registrar of Companies, which is the Director General of the FSC. In addition to public filing requirements relating to shareholders, the FSC requires each company to provide the Commission with details of the ultimate individual beneficial owner of each Jersey-registered company. The Registrar keeps the information in confidence.

The Joint Financial Crime Unit (JFCU), Jersey's financial intelligence unit (FIU), is responsible for receiving, investigating, and disseminating STRs. The unit includes Jersey Police and Customs officers and a financial crime analyst. In 2006, the JFCU received 1,034 STRs. Approximately 25 percent of the STRs filed result in further police investigations. Reports filed in the first six months of 2007 indicate a 32 percent increase in the number of STRs submitted to the JFCU by financial institutions compared to the three-year average for this same period. In the first six months of 2007, Jersey has held more than 2.5 million pounds (approximately $4.9 million) in bank or trust company accounts pending police investigation of suspicious activity. The FIU also responds to requests for financial information from other FIUs. In the first six months of 2007, the JFCU received 219 requests for assistance from counterparts in other jurisdictions.

The Enforcement Division of the Jersey's Financial Services Commission (FSC) responded to 10 requests for assistance from overseas regulators during 2006 and issued public statements concerning nine illegal Internet based businesses that purported to have a Jersey connection. Jersey's law enforcement and regulatory agencies have extensive powers to cooperate with one another, and regularly do so. The FSC cooperates with regulatory authorities, for example, to ensure that financial institutions meet AML obligations.

The JFCU, in conjunction with the Attorney Generals Office, trace, seize and freeze assets. A confiscation order can be obtained if the link to a crime is proven. If the criminal has benefited from a crime, legitimate assets can be forfeited to meet a confiscation order. There is no period of time ascribed to the action of freezing until the assets are released. Frozen assets are confiscated by the

Attorney Generals Office on application to the Court. Proceeds from asset seizures and forfeitures are placed in two funds. Drug-trafficking proceeds go to one fund, and the proceeds of other crimes go to the second fund. The drug-trafficking funds are used to support harm reduction programs, education initiatives, and to assist law enforcement in the fight against drug trafficking. Only limited civil forfeiture is allowed in relation to cash proceeds of drug trafficking located at the ports.

Alternate remittance systems do not appear to be prevalent in Jersey.

The Corruption (Jersey) Law 2005 was passed in alignment with the Council of Europe Criminal Law Convention on Corruption. The new corruption law came into force in February 2007. Articles 2, 3, and 4 of this law were amended in November 2007.

On July 1, 2005, the European Union Savings Tax Directive (ESD) came into force. The ESD is an agreement between the Member States of the European Union (EU) to automatically exchange information with other Member States about EU tax resident individuals who earn income in one EU Member State but reside in another. Although not part of the EU, the three UK Crown Dependencies (Jersey, Guernsey and Isle of Man) have voluntarily agreed to apply the same measures 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, and 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.

Jersey signed the Tax Information Exchange Agreement (TIEA) with the United States in 2002, and plans to sign the same agreements with other countries, thus meeting international obligations to cooperate in financial investigations.

Jersey criminalized money laundering related to terrorist activity with the Prevention of Terrorism (Jersey) Law 1996. The Terrorism (Jersey) Law 2002, which entered into force in January 2003, enhances the powers of the Island authorities to investigate terrorist offenses, to cooperate with law enforcement agencies in other jurisdictions, and to seize assets. Jersey does not circulate the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list, the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224, the EU designated list, or any other government's list. However, Jersey expects its institutions to gather information of designated entities from the Internet and other public sources. Jersey authorities have instituted sanction orders freezing accounts of individuals connected with terrorist activity.

The FSC has reached agreements on information exchange with securities regulators in Germany, France, and the United States. The FSC has a memorandum of understanding for information exchange with Belgium. Registrar information is available, under appropriate circumstances and in accordance with the law, to U.S. and other investigators. In 2007, the FSC has signed a memorandum of understanding with British Virgin Islands Financial Services Commission that will further cooperation between the two regulatory bodies. Application of the 1988 UN Drug Convention was extended to Jersey on July 7, 1997.

Jersey is a member of the Offshore Group of Insurance Supervisors (OGIS) and the Offshore Group of Banking Supervisors (OGBS). It works with the Basel Committee on Banking Supervision and the Financial Action Task Force. The JFCU is a member of the Egmont Group.

The Bailiwick of Jersey should continue to enhance compliance with international standards. Jersey should ensure that all entities, within all sectors, are subject to reporting requirements. The FSC should work to ensure that the AML Unit has enough resources to function effectively, and to provide outreach and guidance to the sectors it regulates. This is especially true for the newest DNFBPs required to file reports. Jersey should mandate the same AML/CTF requirements over its "exempt" companies that it does over the rest of the obliged sectors. The FSC should distribute the UN, European Union and U.S. lists of designated suspected terrorist and terrorist-supporting entities to the obliged entities and not rely on the entities stay current through Internet research.

## Jordan

Jordan is not a regional or offshore financial center and is not considered a major venue for international criminal activity. However, Jordan's long and often remote desert borders and proximity to Iraq make it susceptible to smuggling bulk cash, fuel, narcotics, cigarettes, and other contraband. The influx of refugees has caused an increase in cross border criminal activity. Jordan boasts a thriving "import-export" community of brokers, traders, and entrepreneurs that regionally are involved with value transfer via trade and customs fraud.

In August 2001, the Central Bank of Jordan, which regulates banks and financial institutions, issued anti-money laundering regulations designed to meet some of the Financial Action Task Force (FATF) Forty Recommendations on Money Laundering. Since that time, money laundering has been considered an "unlawful activity" subject to criminal prosecution. After the lifting of Iraqi sanctions, there have been few reports of money laundering through Jordanian banks. On July 17, 2007, Jordan enacted a comprehensive anti-money laundering law (AML). The law, Law No. 46 for the Year 2007, created a committee known as the National Committee on Anti-Money Laundering (NCAML). The committee is chaired by the Governor of the Central Bank of Jordan and has as members: the Deputy Governor of the Central Bank named by the Governor of the Central Bank to serve as deputy chairman of the committee, the Secretary General of the Ministry of Justice, the Secretary General of the Ministry of the Interior, the Secretary General of the Ministry of Finance, the Secretary General of the Ministry of Social Development (which overseas charitable organizations), the Director of the Insurance Commission, the Controller General of Companies, a Commissioner of the Securities Commission, and the head of the Anti-Money Laundering Unit. The Anti-Money Laundering Unit (AMLU), formerly the Central Bank's Suspicious Transaction Follow-Up Unit, was formed immediately on passage of the law and designated as the Government of Jordan's (GOJ) financial intelligence unit (FIU). The AMLU is staffed with a director, outreach officer, chief counsel, and one analyst. It is anticipated that during 2008, the unit's staff will be augmented to include a minimum of seven analysts and liaison personnel from the two national law enforcement agencies, public prosecutors, and other regulatory entities.

The AMLU is designated as an independent entity, but is housed at present in the Central Bank of Jordan. It is organized on a general administrative FIU model. It is responsible for receiving suspicious activity reports (SARs) from obligated entities designated in the law, analyzing them, requesting additional information related to the activity and reporting it to the prosecutor general for further action. Involvement of the AMLU in assisting criminal investigations is dependent on public prosecutors. At the end of 2007, the AMLU was working to establish formal ties through memoranda of understanding with competent GOJ authorities possessing the necessary databases and resources pertinent to pursuing financial intelligence analysis and money laundering investigations.

The 2007 AML law criminalizes money laundering and stipulates as predicate offenses any felony crime or any crime stated in international agreements to which Jordan is a party, whether such crimes are committed inside or outside the Kingdom, provided that the act committed is subject to penalty in the country in which it occurs. The Central Bank of Jordan previously instructed financial institutions

to be particularly careful when handling foreign currency transactions, especially if the amounts involved are large or if the source of funds is in question. The new law requires obligated entities to: undertake due diligence in identifying customers; refrain from dealing with anonymous persons or shell banks; report to the AMLU any suspicious transaction, completed or not; and comply with instructions issued by competent regulatory parties to implement provisions of the law. The Ministries of Justice, Interior, Finance, and Social Development, as well as the Insurance Commission, Controller General of Companies, and Securities Commission all have a part in regulating various other nonfinancial institutions through issued regulations and instructions. The AMLU is obligated to work with these entities to ensure that a comprehensive approach to AML/CTF is undertaken in keeping with international standards and best practices.

Financial institutions are required under the new law to report all suspicious transactions whether the transaction was completed or not. This includes banks, foreign exchange companies, money transfer companies, stock brokerages, insurance companies, credit companies, and any company whose articles of association state that their activities include debt collection and payment services, leasing services, investment and financial asset management, real estate trading and development, and trading in precious metals and stones. Lawyers and accountants are not considered to be obligated entities under the law.

All obligated entities are required to conduct due diligence to identify customers, their activities, legal status, and beneficiaries and follow-up on transactions that are conducted through an ongoing relationship. Business dealings with anonymous persons, persons using fictitious names or shell banks are prohibited. Obligated entities are required to comply with instructions issued by competent regulatory authorities as listed in the law. Disclosure to the customer or the customer's beneficiary of STRs and/or verifications or investigations by competent authorities is prohibited. They are also required to respond to any inquiry from the AMLU regarding STRs or requests for assistance from other competent judicial, regulatory, administrative, or security authorities needing information to perform their responsibilities.

Jordanian officials report that financial institutions file suspicious transaction reports and cooperate with prosecutors' requests for information related to narcotics trafficking and terrorism cases. The AMLU received over 30 SARs in 2007, two of which were forwarded for prosecution. There were no arrests or convictions for money laundering or terrorist financing in Jordan in 2007. The standard for forwarding SARs is potentially a problem in the existing law.

The Banking Law of 2000 (as amended in 2003) allows judges to waive bank secrecy provisions in any number of criminal cases, including suspected money laundering and terrorist financing. An October 8, 2001 revision to the Penal Code criminalized terrorist activities, specifically financing of terrorist organizations. Guidelines issued by the Central Bank state that banks should research all sanctions lists relating to terrorist financing including those issued by individual countries and other relevant authorities. The Central Bank may not circulate names on sanctions lists to banks unless the names are included on the UNSCR 1267 Sanctions Committee's consolidated list. No such assets have been identified to date. Banks and other financial institutions are required to maintain records for a period of five years.

One significant challenge facing the GOJ is determining which law enforcement entity will be tasked to conduct financial investigations relating to AML/CTF. Since the AML law was only implemented in July 2007, law enforcement agencies and public prosecutors are still deliberating the issue.

There are six public free trade zones in Jordan: the Zarqa Free Zone, the Sahab Free Zone, the Queen Alia International Airport Free Zone; the Al-Karak Free Zone, the Al-Karama Free Zone and the Aqaba Free Zone. All of the six list their investment activities as "industrial, commercial, service, and touristic." There are 32 private free trade zones, a number of which are related to the aviation industry. Other free trade zones list their activities as industrial, agricultural, pharmaceutical, training of human

capital, and multi-purpose. All free trade zones are regulated by the Jordan Free Zones Corporation in the Ministry of Finance and are guided by the Law of Free Zones Corporation No. 32 for 1984 (and amendments). Regulations state that companies and individuals using the zones must be identified and registered with the Corporation.

Although the 2007 AML law requires reporting of cross-border movement of money if the value exceeds a threshold amount set by the NCAML, no threshold amount was set by the end of 2007. The law also provides for the creation of cross-border currency and monetary instruments declaration forms, and the AMLU is working on the creation of the form. However, the declaration requirement applies only for the entry of money into the Kingdom and not outgoing. The Customs Department is responsible for archiving the declaration forms once implemented. In December 2004, the United States and Jordan signed an Agreement regarding Mutual Assistance between their Customs Administrations that provides for mutual assistance with respect to customs offenses and the sharing and disposition of forfeited assets. The AML law authorizes Customs "to seize or restrain" undeclared money crossing the border and report same to the AMLU which will decide whether the money should be returned or the case referred to the judiciary.

Jordan 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 Corruption. Jordan has signed but has yet to ratify the UN Convention against Transnational Organized Crime. Jordan is a charter member of the Middle East and North Africa Financial Action Task Force (MENAFATF) and in 2007 Jordan held the presidency of MENAFATF. Jordan's AMLU aspires to membership in the Egmont Group of Financial Intelligence Units.

The new AML law provides judicial authorities the legal basis to cooperate with foreign judicial authorities in providing assistance in foreign investigations, extradition, and freezing and seizing of funds related to money laundering in accordance with current legislation and bilateral or multilateral agreements to which Jordan is a part based on reciprocity. Judicial authorities may order implementation of requests by foreign judicial authorities to confiscate proceeds of crime relating to money laundering and to distribute such proceeds in accordance with bilateral or multilateral agreements. Jordan's Anti-drugs Law allows the courts to seize proceeds of crime derived from acts proscribed by the law. The Economic Crimes Law gives both prosecutors and the courts the authority to seize the assets of any person who has committed a crime under that law for a period of three months while an investigation is underway. Jordan's penal code further provides prosecutors the authority to confiscate "all things" derived from a felony or intended misdemeanor.

In light of the 2007 AML law, the Government of Jordan's NCAML and the AMLU should conduct a comprehensive evaluation of Jordan's capabilities in preventing money laundering and enforcing its new law in accordance with international standards and best practices. Jordanian law enforcement and customs should examine forms of bulk cash smuggling relating to terrorist financing and trade-based money laundering and incorporate prevention and investigative strategies that meet the requirements of complex financial investigations. The GOJ should ratify the UN Convention against Transnational Organized Crime.

## Kenya

Kenya is developing into a major money laundering country. As a regional financial and trade center for Eastern, Central, and Southern Africa, Kenya's economy has large formal and informal sectors. Kenya's use as a transit point for international drug traffickers is increasing. Domestic drug abuse is also increasing, especially in Coast Province. Narcotics proceeds are being laundered in Kenya, although the volume has not yet been determined. Kenya has no offshore banking or Free Trade Zones. There is no significant black market for smuggled goods in Kenya. However, Kenya serves as the major transit country for Uganda, Tanzania, Rwanda, Burundi, northern Democratic Republic of

Congo (DRC), and Southern Sudan. Goods marked for transit to these northern corridor countries avoid Kenyan customs duties, but have been known to be sold in Kenya.

Many entities in Kenya are involved in exporting and importing goods, including a reported 800 registered, international nongovernmental organizations (NGOs) managing over U.S. $1 billion annually. International organizations operating in the conflict areas of the region—Southern Sudan, Somalia, Burundi and DRC—keep all their dollars in Kenyan banks.

Annual remittances from expatriate Kenyans are estimated at U.S. $680-780 million. Individual Kenyans and foreign residents also transfer money in and out of Kenya. Nairobi's Eastleigh Estate has become an informal hub for remittances by the Somalia Diaspora, transmitting millions of dollars every day from Europe, Canada and the U.S. to Mogadishu. Many transfers are executed via formal channels such as wire services and banks, but there is also a thriving network of cash-based, unrecorded transfers that the Government of Kenya (GOK) cannot track. Expatriates primarily use this system to send and receive remittances internationally. The large Somali refugee population in Kenya uses a hawala system to send and receive remittances. The GOK has no means to monitor hawala transfers. Kenya does not have an effective legal regime to address money laundering. The GOK has no regulations to freeze/seize criminal or terrorist accounts, and has not passed a law that explicitly outlaws money laundering and creates a financial intelligence unit (FIU).

Section 49 of the Narcotic Drugs and Psychotropic Substance Control Act of 1994 criminalizes money laundering related to narcotics trafficking. The offense is punishable by a maximum prison sentence of 14 years. However, Kenya has never seen a conviction for the laundering of proceeds from narcotics trafficking. Money laundering is a criminal offense, through a patchwork of laws and guidance that the GOK has cobbled together, including the 1994 Act, Legal Notice No. 4 of 2001, the Central Bank of Kenya (CBK) Guidelines on Prevention of Money Laundering, and enabling provisions of other laws. Kenya has not developed an effective anti-money laundering (AML) regime.

In November 2006, the GOK published a proposed Proceeds of Crime and Anti-Money Laundering Bill, a revised version of a 2004 law. The proposed law declares itself to be "An act of Parliament to provide for the offence of money laundering and to introduce measures for combating the offence, to provide for the identification, tracing, freezing, seizure and confiscation of the proceeds of crime." It defines "proceeds of crime" as any property or economic advantage derived or realized, directly or indirectly, as a result of or in connection with an offence. The draft legislation provides for criminal and civil restraint, seizure and forfeiture. In addition, the proposed bill authorizes the establishment of an FIU and requires financial institutions and nonfinancial businesses or professions, including casinos, real estate agencies, precious metals and stones dealers, and legal professionals and accountants, to file suspicious transaction reports above a certain threshold. The bill also identifies 30 other statutes for the GOK to amend so that they will be consistent with the bill when it is passed.

This bill has deficiencies. It does not mention terrorism, nor does it specifically define "offense" or "crime." The proposed legislation does not explicitly authorize the seizure of legitimate businesses used to launder money. The requirement that only suspicious transactions above a certain threshold are reported is inconsistent with international standards, which call for suspicious transaction reports to have no monetary threshold. The GOK tabled the bill in Parliament in November 2007, but Parliament never took the bill up, and it lapsed when Parliament recessed on December 8. The government will need to republish and resubmit the bill in the Tenth Parliament in 2008.

The CBK is the regulatory and supervisory authority for Kenya's deposit-taking institutions and has oversight for more than 50 such entities, as well as mortgage companies and other financial institutions. The Minister of Home Affairs supervises casinos, although its regulation of this sector is ineffective.

CBK regulations require deposit-taking institutions to verify the identity of new customers opening an account or conducting a transaction. The Banking Act amendment of December 2001 authorizes the CBK to disclose financial information to any monetary or financial regulatory authority within or outside Kenya. In 2002, the Kenya Bankers Association (KBA) issued guidelines requiring banks to report suspicious transactions to the CBK. These guidelines do not have the force of law, and only a handful of suspicious transactions have been reported so far. Under the regulations, banks must maintain records of transactions over U.S. $100,000 and international transfers over U.S. $50,000, and report them to the CBK. A law enforcement agency can demand information from any financial institution, if it has obtained a court order. Some commercial banks and foreign exchange bureaus file suspicious transaction reports voluntarily, but they run the risk of civil litigation, as there are no adequate "safe harbor" provisions for reporting such transactions to the CBK. A court ruling to penalize a commercial bank in 2002 for disclosing information to the CBK in response to a court order, made banks wary of reporting suspicious transactions. In a November 2007 decision that will likely further chill banks' willingness to report suspicious transactions, a judge ordered Barclays Bank to pay a customer Kenya Shillings (Sh) 400,000 (approximately U.S. $6,107) for violating confidentiality by providing details on the customer's specimen signature to the British High Commission without her consent for processing a visa application.

These regulations do not cover nonbank financial institutions such as money remitters, casinos, or investment companies, and there is no enforcement mechanism behind the regulations. Kenya lacks the institutional capacity, investigative skill and equipment to conduct complex investigations independently. There have been no arrests or prosecutions for money laundering or terrorist financing.

There are 95 foreign exchange bureaus under GOK supervision. The Central Bank of Kenya Act (Cap 491) regulates forex bureaus, which are authorized dealers of currency. The CBK subsequently recognized that several bureaus violated the Forex Bureau Guidelines, including dealing in third party checks and executing telegraphic transfers without CBK approval. The checks and transfers may have been used for fraud, tax evasion and money laundering. In response, the CBK's Banking Supervision Department issued Central Bank Circular No. 1 of 2005 instructing all forex bureaus to immediately cease dealing in telegraphic transfers and third party checks. These new guidelines, which fall under Section 33K of the Central Bank of Kenya Act, took effect on January 1, 2007.

Kenya has little in the way of cross-border currency controls. GOK regulations require that any amount of cash above U.S. $5,000 be disclosed at the point of entry or exit for record-keeping purposes only, but this provision is rarely enforced, and authorities keep no record of cash smuggling attempts. The CBK guidelines call for currency exchange bureaus to furnish daily reports on any single foreign exchange transaction above U.S. $10,000, and on cumulative daily foreign exchange inflows and outflows above U.S. $100,000. Guidelines require that foreign exchange dealers ensure that cross-border payments have no connection to illegal financial transactions.

Recent investigations illustrate Kenya's vulnerability to money laundering. The Charterhouse Bank investigations in 2006 and 2007 revealed that the proceeds of large-scale evasion of import duties and taxes had been laundered through the banking system since at least 1999. In addition, the smuggled and/or under-invoiced goods may have also been marketed through the normal wholesale and retail sectors. Charterhouse Bank managers had conspired with depositors to evade import duties and taxes and launder the proceeds totaling approximately $500 million from 1999 to 2006. In June 2006, a Member of Parliament tabled a 2004 initial investigation report on Charterhouse Bank by a special CBK investigations team indicating account irregularities, tax evasion and money laundering by some of the bank's clients. The Ministry of Finance temporarily closed the bank to prevent a run, and the CBK placed Charterhouse Bank under statutory management to preserve records and prevent removal of funds. Subsequent audits and investigations covering the period 1999-2006 found that Charterhouse Bank had violated the CBK's know-your-customer procedures in over 80 percent of its accounts, and were missing basic details such as the customer's name, address, ID photo, or signature cards.

Charterhouse Bank also violated the Banking Act and the CBK's Prudential Guidelines by not properly maintaining records for foreign currency transactions. Available evidence makes clear that the bank management had, on a large scale, consistently evaded and ignored normal internal controls by allowing many irregular activities to occur. The bank management's continual violation of CBK prudential guideline CBK/PG/08 requirements to report suspicious transactions, and its efforts to conceal them from CBK examiners, also indicate that bank officials were complicit in these suspicious transactions. The perpetrators demonstrated an understanding of AML controls, transferring funds to the United States and the United Kingdom in increments just below reporting thresholds of the receiving banks for large currency transactions. The Minister of Finance advised Charterhouse and the CBK that the Ministry would not renew the bank's license to operate after December 31, 2006. (Bank licenses are annual and expire automatically at the end of each year if not renewed.) The courts rejected Charterhouse owners' legal challenges, and the bank remained closed.

This case illustrates that criminals have been taking advantage of Kenya's inadequate AML regime for years by evading oversight and/or by reportedly paying off enforcement officials, other government officials, and politicians. There are strong indications that other Kenyan banks are also involved in similar activities. Reportedly, Kenya's financial system may be laundering over U.S. $100 million each year. However, in 2006 and 2007 there were not any reported money laundering related arrests, prosecutions, or convictions.

Kenya has not criminalized the financing of terrorism as required by the United Nations Security Council Resolution 1373 and the UN International Convention for the Suppression of Financing of Terrorism, to which it is a party. In April 2003, the GOK introduced the Suppression of Terrorism Bill into Parliament. After objections from some public groups that the bill unfairly targeted the Muslim community and unduly restricted civil rights, the GOK withdrew the bill. The GOK drafted the Anti-Terrorism Bill in 2006, which contains provisions that would strengthen the GOK's ability to combat terrorism. It also revises the controversial text, but Muslim and human rights groups remain convinced the government could use it to commit human rights violations. The GOK published the bill and submitted it to Parliament in 2007, but Parliament took no action and the bill will have to be resubmitted to the tenth Parliament in 2008.

The GOK requires all charitable and nonprofit organizations to register with the government and submit annual reports to the GOK's oversight body, the National Non-Governmental Organization Coordination Bureau. NGOs that are noncompliant with the annual reporting requirements can have their registrations revoked; however, the government rarely imposes such penalties. The GOK revoked the registration of some NGOs with Islamic links in 1998 after the bombing of the U.S. Embassy in Nairobi, only to later re-register them. The Non-Governmental Organization Coordination Bureau lacks the capacity to monitor NGOs, and observers suspect that charities and other nonprofit organizations handling millions of dollars are filing inaccurate or no annual reports. The Bureau made some progress towards strengthening its capacity to review NGO registrations and annual reports for suspicious activities in 2007.

Drug trafficking-related asset seizure and forfeiture laws and their enforcement are weak and disjointed. With the exception of intercepted drugs and narcotics, seizures of assets are rare. At present, the government entities responsible for tracing and seizing assets are the Central Bank of Kenya Banking Fraud Investigation Unit, the Kenya Police Anti-Narcotics and Anti-Terrorism Police Units, the Kenya Revenue Authority (KRA), and the Kenya Anti-Corruption Commission (KACC). To demand bank account records or to seize an account, the police must present evidence linking the deposits to a criminal violation and obtain a court warrant. This process is difficult to keep confidential, and as a result of leaks, serves to warn account holders of investigations. Account holders then move their accounts or contest the warrants.

The CBK does not circulate the list of individuals and entities on the United Nations (UN) 1267 Sanctions Committee's consolidated list or the United States Office of Foreign Asset Control (OFAC) designated list to the financial institutions it regulates. Instead, the CBK uses its bank inspection process to search for names on the OFAC list of designated people and entities. The CBK and the GOK have no authority to seize or freeze accounts without a court warrant. To date, the CBK has not notified the United States Government of any bank customers identified on the OFAC list. There is currently no law specifically authorizing the seizure of the financial assets of terrorists.

Kenya 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. Kenya ranks 150 out of 180 countries on the 2007 Transparency International Corruption Perceptions Index. Kenya is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a Financial Action Task Force (FATF)-style regional body. Kenya has an informal arrangement with the United States for the exchange of information relating to narcotics, terrorist financing, and other serious crime investigations. Kenya has cooperated with the United States and the United Kingdom.

The GOK should criminalize the financing of terrorism and pass a law authorizing the government to seize the financial assets of terrorists and convict individuals or groups that finance terrorist activity. Kenyan authorities should take steps to ensure that NGOs and suspect charities and nonprofit organizations follow internationally recognized transparency standards and file complete and accurate annual reports. The GOK should pass and enact the proposed Proceeds of Crime and Anti-Money Laundering bill, including the creation of an FIU. The CBK, law enforcement agencies, and the Ministry of Finance should improve coordination to enforce existing laws and regulations to combat money laundering, tax evasion, corruption, and smuggling. The Minister of Finance should revoke or refuse to renew the license of any bank found to have knowingly laundered money, and encourage the CBK to tighten its examinations and audits of banks. Kenyan law enforcement should be more proactive in investigating money laundering and related crimes, and customs should exert control of Kenya's borders.

## Korea, Democratic Peoples Republic of

For decades, citizens of the Democratic People's Republic of Korea (DPRK) have been apprehended in international investigations trafficking in narcotics and other forms of criminal behavior, including passing counterfeit U.S. currency (including U.S. $100 "super notes") and trading in counterfeit products, such as cigarettes and pharmaceuticals. There is substantial evidence that North Korean governmental entities and officials have been involved in the laundering of the proceeds of narcotics trafficking and other illicit activities and that they continue to be engaged in counterfeiting and other illegal activities through a number of front companies. The illegal revenue provides desperately needed hard currency for the economy of the DPRK. On October 25, 2006 the Standing Committee of the Supreme People's Assembly of the DPRK adopted a law "On the Prevention of Money Laundering." The law states the DPRK has made it its "consistent policy to prohibit money laundering," but the law is significantly deficient in most important respects and there is no evidence that it has been implemented.

On September 15, 2005, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) designated Macau-based Banco Delta Asia (BDA) as a primary money laundering concern under Section 311 of the USA PATRIOT Act and issued a proposed rule regarding the bank, citing the bank's systemic failures to safeguard against money laundering and other financial crimes. In its designation of BDA as a primary money laundering concern, FinCEN cited in the Federal Register that "the involvement of North Korean Government agencies and front companies in a wide variety of illegal activities, including drug trafficking and the counterfeiting of goods and currency"

and noted that North Korea has been positively linked to nearly 50 drug seizures in 20 different countries since 1990. Treasury finalized the Section 311 rule in March 2007, prohibiting U.S. financial institutions from opening or maintaining correspondent accounts for or on behalf of BDA. This rule remains in effect. Following the Section 311 designation of BDA, the Macau Monetary Authority (MMA) froze approximately U.S. $25 million in North Korean-related accounts at the bank. The MMA subsequently lifted the freeze on these funds following the issuance of the final rule.

The DPRK became a party to the 1988 UN Drug Convention during 2007. It still is not a party to the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, or the UN International Convention for the Suppression of the Financing of Terrorism. North Korea is not a participant in any FATF-style regional body. The DPRK should develop a viable anti-money laundering/counter-terrorist financing regime that comports with international stands. The U.S. Department of State has designated North Korea as a State Sponsor of Terrorism.

## Korea, Republic of

The Republic of Korea (ROK) has not been considered an attractive location for international financial crimes or terrorist financing due to foreign exchange controls that are gradually being phased out by 2009. Most money laundering appears to be associated with domestic criminal activity or corruption and official bribery. Laundering the proceeds from illegal game rooms, customs fraud, exploiting zero VAT rates applied to gold bars, trade-based money laundering, counterfeit goods and intellectual property rights violations are all areas of concern. Moreover, criminal groups based in South Korea maintain international associations with others involved in human trafficking, contraband smuggling and related organized crime. As law enforcement authorities have gained more expertise investigating money laundering and financial crimes, they have become more cognizant of the problem.

On the whole, the South Korean government has been a willing partner in the fight against financial crime, and has pursued international agreements toward that end. The Financial Transactions Reports Act (FTRA), passed in September 2001, requires financial institutions to report suspicious transactions to the Korea Financial Intelligence Unit (KoFIU), which operates within the Ministry of Finance and Economy. The KoFIU was officially launched in November 2001, and is composed of 60 experts from various agencies, including the Ministry of Finance and Economy, the Justice Ministry, the Financial Supervisory Commission, the Bank of Korea, the National Tax Service, the National Police Agency, and the Korea Customs Service. KoFIU analyzes suspicious transaction reports (STRs) and forwards information deemed to require further investigation to the Public Prosecutor's office, and, as of 2007, also to the Korean police. The Financial Transaction Reporting Act Amendment Bill was submitted to the National Assembly in January 2007. If passed, this bill will expand the coverage of AML measures to nonfinancial businesses and professions, including casinos, and require financial institutions to file an STR when it is suspected that those funds are related to terrorism.

In 2007, the KoFIU upgraded its anti-money-laundering monitoring system by introducing the Korea Financial Intelligence System based on scoring and data mining methods, in addition to continued Suspicious Transaction Reports (STR), Currency Transaction Reports (CTR) and Customer Due Diligence (CDD) reports. Beginning in January 2006, financial institutions have been required to report within 24 hours all cash transactions of 50 million Korean won (approximately U.S. $54,350) or more by individuals to KoFIU. That reporting threshold will be lowered to 30 million won (approximately U.S. $32,610) in 2008 and to 20 million won (approximately U.S. $21,740) in 2010. Since January 2006, financial institutions have also been required to perform enhanced customer due diligence, thereby strengthening customer identification requirements set out in the Real Name Financial Transaction and Guarantee of Secrecy Act. Under the enhanced due diligence guidelines, financial institutions must identify and verify customer identification data, including address and telephone numbers, when opening an account or conducting transactions of 20 million won or more.

The STR system was strengthened in 2004 with the introduction of a new online electronic reporting system and the lowering of the monetary threshold under which financial institutions must file STRs from 50 to 20 million won. Reporting entities may file STRs regarding transactions below this threshold. In addition, KoFIU announced that it would consider lowering or removing the threshold for obligatory STR reporting. Improper disclosure of financial reports is punishable by up to five years imprisonment and a fine of up to 30 million won. Between January 1, 2002, and September 30, 2007, KoFIU received a total of 80,417 STRs from financial institutions. The number of such cases has continued to climb noticeably each year, from 275 STRs in 2002, to 1,744 in 2003, 4,680 in 2004, 13,459 in 2005, and 24,149 in 2006. In the first nine months of 2007, there were 36,110 STRs submitted to KoFIU, a 120 percent increase over the same period in 2006. Since 2002 through the end of September 2007, KoFIU has analyzed 79,325 of these reports and provided 7,184 reports to law enforcement agencies, including the Public Prosecutor's Office (PPO), National Police Agency (NPA), National Tax Service (NTS), Korea Customs Service (KCS), and the Financial Supervisory Commission (FSC). Of the 7,184 cases referred to law enforcement agencies, investigations have been completed in 3,661 cases, with 1,402 cases resulting in indictments and prosecutions for money laundering.

In addition, KoFIU supervises and inspects the implementation of internal reporting systems established by financial institutions and is charged with coordinating the efforts of other government bodies. Officials charged with investigating money laundering and financial crimes are beginning to widen their scope to include crimes related to commodities trading and industrial smuggling, and continue to search for possible links of such illegal activities to international terrorist activity. In 2007, KoFIU continued to strengthen advanced anti-money laundering measures (such as the STR and CTR systems), and became an observer to the Financial Action Task Force (FATF) in July 2006. The KoFIU also encouraged financial institutions including small-scale credit unions and cooperatives to adopt a differentiated risk-based due diligence system, focusing on types of customers and transactions, by offering them comprehensive training programs.

Money laundering controls are applied to nonbanking financial institutions, such as exchange houses, stock brokerages, casinos, insurance companies, merchant banks, mutual savings, finance companies, credit unions, credit cooperatives, trust companies, and securities companies. Following the late-2005 arrest of a Korean business executive charged with laundering 8.3 billion won (U.S. $8.17 million) to be used to bribe politicians and bureaucrats, the KoFIU in January 2007 submitted to the National Assembly a revision bill of the Financial Transaction Reports Act to impose anti-money laundering obligations on casinos. KOFIU plans to expand the obligation to intermediaries such as lawyers, accountants, or broker/dealers, currently not covered by Korea's money laundering controls. Any traveler carrying more than U.S. $10,000 or the equivalent in other foreign currency is required to report the currency to the Korea Customs Service.

Money laundering related to narcotics trafficking has been criminalized since 1995, and financial institutions have been required to report transactions known to be connected to narcotics trafficking to the Public Prosecutor's Office since 1997. All financial transactions using anonymous, fictitious, and nominee names have been banned since the 1997 enactment of the Real Name Financial Transaction and Guarantee of Secrecy Act. The Act also requires that, apart from judicial requests for information, persons working in financial institutions are not to provide or reveal to others any information or data on the contents of financial transactions without receiving a written request or consent from the parties involved. However, secrecy laws do not apply when such information must be provided for submission to a court or as a result of a warrant issued by the judiciary.

In a move designed to broaden its anti-money laundering regime, the ROK also criminalized the laundering of the proceeds from 38 additional offenses, including economic crimes, bribery, organized crime, and illegal capital flight, through the Proceeds of Crime Act (POCA), enacted in September 2001. The POCA provides for imprisonment and/or a fine for anyone receiving, disguising, or

disposing of criminal funds. The legislation also provides for confiscation and forfeiture of illegal proceeds.

South Korea still lacks specific legislation on terrorist financing although, as noted above, the Suppression of the Financing of Terrorism Bill was submitted to the National Assembly in January 2007. As of December 2007, three versions of the new counter-terrorism bill were pending in Korea's unicameral legislature, the National Assembly. The proposed Suppression of the Financing of Terrorism bill is crafted to allow the Korean Government additional latitude in fighting terrorism The Suppression of the Financing of Terrorism bill would also permit the government to seize legitimate businesses that support terrorist activity. Currently, under the special act against illicit drug trafficking and other related laws, legitimate businesses can be seized if they are used to launder drug money, but businesses supporting terrorist activity cannot be seized unless other crimes are committed.

Previous attempts to pass similar CTF legislation have not succeeded. Many politicians and nongovernmental organizations (NGOs), recalling past civil rights abuses in Korea by former administrations, oppose the passage of counterterrorism legislation because of fears about possible misuse by the National Intelligence Service and other government agencies.

If passed, the new laws amending the Financial Transactions Reporting Act and the bill Suppression of the Financing of Terrorism would not be enforceable for 12 months. Moreover, the legislation would not correct some potential shortcomings regarding key elements on the criminalization of terrorist financing and suspicious transaction reporting-including excessively high thresholds for reporting all types of suspicious activity. In addition, they may leave some gaps on existing requirements to identify beneficial owners.

Through KoFIU, the government circulates to its financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list, the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224, and those listed by the European Union under relevant authorities. Korea implemented regulations on October 9, 2001, to freeze financial assets of Taliban-related authorities designated by the UN Security Council. The government then revised the regulations, agreeing to list immediately all U.S. Government-requested terrorist designations under U.S. Executive Order 13224 of December 12, 2002. No listed terrorists are known to be maintaining financial accounts in Korea and there have been no cases of terrorist financing identified since 2002.

Korean government authorities continue to investigate the underground "hawala" system used primarily to send illegal remittances abroad by South Korea's approximately 30,000 foreigners from the Middle East as well as thousands of undocumented foreign workers (mainly ethnic Koreans from Mongolia, Uzbekistan, and Russia). Currently, gamblers who bet abroad often use alternative remittance and payment systems; however, government authorities have criminalized those activities through the Foreign Exchange Regulation Act and other laws. According to an October 2007 report by the Korea Customs Service, there were 1,311 investigations into underground remittances amounting to 2.2 trillion won (approximately U.S. $1.84 billion) in 2003, 1,917 cases totaling 3.66 trillion won (approximately U.S. $3.2 billion) in 2004, 1,901 cases worth 3.56 trillion won (approximately U.S. $3.47 billion) in 2005, 1,924 cases totaling 2.7 trillion (approximately U.S. $2.8 billion) in 2006, and 1,199 cases totaling 1.2 trillion won (approximately U.S. $1.3 billion) in the first half of 2007. The majority of early underground remittance cases were related to the U.S. through 2004; but between 2005 and June 2007, the bulk of cases involved China (35.4 percent, approximately U.S. $2.87 billion), followed by Japan (34.9 percent, approximately U.S. $2.83 billion) and the U.S. (18 percent, U.S. $1.46 billion).

South Korea actively cooperates with the United States and other countries to trace and seize assets. The Anti-Public Corruption Forfeiture Act of 1994 provides for the forfeiture of the proceeds of assets derived from corruption. In November 2001, Korea established a system for identifying, tracing,

freezing, seizing, and forfeiting narcotics-related and/or other assets of serious crimes. Under the system, KoFIU is responsible for analyzing and providing information on STRs that require further investigation. The Bank Account Tracing Team under the Narcotics Investigation Department of the Seoul District Prosecutor's Office (established in April 2002) is responsible for tracing and seizing drug-related assets. The Korean Government established six additional new bank account tracking teams in 2004 to serve out of the District Prosecutor's offices in the metropolitan cities of Busan, Daegu, Kwangju, Incheon, Daejon, and Ulsan, to expand its reach. Its legal framework does not allow civil forfeiture.

Korea continues to address the problem of the transportation of counterfeit international currency. The Bank of Korea reported that through September 2007, there were 518 reported cases of counterfeit dollars worth U.S. $1,052,050. Bank experts confirm that the amount of forged U.S. currency is on a decline.

South Korea has a number of free economic zones (FEZs) that enjoy certain tax privileges. However, companies operating within them are subject to the same general laws on financial transactions as companies operating elsewhere, and there is no indication these FEZs are being used in trade-based money laundering schemes or for terrorist financing. Korea mandates extensive entrance screening to determine companies' eligibility to participate in FEZ areas, and firms are subject to standard disclosure rules and criminal laws. In 2007 Korea had seven FEZs, as a result of the June 2004 re-categorization of the three port cities of Busan, Incheon, and Kwangyang as FEZs. They were re-categorized from their previous designation of "customs-free areas" to avoid confusion from the earlier dual system of production-focused FEZs, and logistics-oriented "customs-free zones." Incheon International Airport is slated to become the eighth FEZ.

Korea is a party to the 1988 UN Drug Convention and, in December 2000, signed, but has not yet ratified, the UN Convention against Transnational Organized Crime. Korea is a party to the UN International Convention for Suppression of the Financing of Terrorism. The ROK also signed in December 2003, but has not ratified, the UN Convention against Corruption. Korea is an active member of the Asia/Pacific Group on Money Laundering (APG). Korea also became a member of the Egmont Group in 2002. An extradition treaty between the United States and the ROK entered into force in December 1999. The United States and the ROK cooperate in judicial matters under a Mutual Legal Assistance Treaty, which entered into force in 1997. In addition, the FIU continues to actively pursue information-sharing agreements with a number of countries, and had signed memoranda of understanding with 34 countries-the latest being Malaysia-in April 2007.

The Government of Korea should continue to move forward to adopt and implement its pending counter-terrorism legislation and amendments to the Financial Transaction Reporting Act. Among other priorities, the government should extend its anti-money laundering regime to intermediaries such as lawyers, accountants, broker/dealers and informal lending widely recognized as potential blind spots. Korea should lower the high monetary threshold for reporting suspicious transactions and extend the reporting obligation to attempted transactions. The Republic of Korea should continue its policy of active participation in international anti-money laundering efforts, both bilaterally and in multilateral fora. Spurred by enhanced local and international concern, Korean law enforcement officials and policymakers now understand the potential negative impact of such activity on their country, and have begun to take steps to combat its growth. Their efforts will become increasingly important due to the rapid growth and greater integration of Korea's financial sector into the world economy.

## Kuwait

Kuwait continues to experience unprecedented economic growth that is enhancing the country's regional financial influence, which may make the market susceptible to money laundering. However,

money laundering is not believed to be a significant problem, and reportedly that which does take place is generated largely as revenues from drug and alcohol smuggling into the country and the sale of counterfeit goods. However, Kuwait-based terrorist financing, specifically the ongoing threat of charity misuse, continues to be a concern.

Kuwait has ten private local commercial banks, including three Islamic banks, all of which provide traditional banking services comparable to Western-style commercial banks. Kuwait also has one specialized bank, the government-owned Industrial Bank of Kuwait, which provides medium and long-term financing. The three Islamic banks are the Kuwait Finance House (KFH), Boubyan Islamic Bank, and the Kuwait Real Estate Bank (KREB).

The Kuwaiti banking sector was opened to foreign competition in 2001 under the Direct Foreign Investment Law. The Central Bank of Kuwait (CBK) has granted licenses to five foreign banks: BNP Paribas, HSBC, Citibank, the National Bank of Abu Dhabi, and Qatar National Bank. However, the National Bank of Abu Dhabi and Qatar National Bank have not opened offices. Although foreign banks may operate in Kuwait, they are limited to one branch each.

On March 10, 2002, the Emir (Head of State) of Kuwait signed Law No. 35/2002, commonly referred to as Law No. 35, which criminalized money laundering. Law 35 does not criminalize terrorist financing. The law stipulates that banks and financial institutions may not keep or open anonymous accounts or accounts in fictitious or symbolic names and that banks must require proper identification of both regular and occasional clients. The law also requires banks to keep all records of transactions and customer identification information for a minimum of five years, conduct anti-money laundering and terrorist financing training to all levels of employees, and establish proper internal control systems.

Law No. 35 also requires banks to report suspicious transactions to the Office of Public Prosecution (OPP). The OPP is the sole authority that has been designated by law to receive suspicious transaction reports (STRs) and to take appropriate action on money laundering operations. Reports of suspicious transactions are then referred to the CBK for analysis. The anti-money laundering law provides for a penalty of up to seven years imprisonment in addition to fines and asset confiscation. The penalty is doubled if an organized group commits the crime, or if the offender took advantage of his influence or his professional position. Moreover, banks and financial institutions may face a steep fine (approximately $3.3 million) if found in violation of the law.

The law includes articles on international cooperation and the monitoring of cash and precious metals transactions. Currency smuggling into Kuwait is also outlawed under Law No. 35, although cash reporting requirements are not uniformly enforced at ports of entry. Provisions of Article 4 of Law No. 35 require travelers to disclose any national or foreign currency, gold bullion, or other precious materials in their possession valued in excess of 3,000 Kuwaiti dinars (approximately U.S. $10,000) to customs authorities upon entering the country. However, the law does not require individuals to file declaration forms when carrying cash or precious metals out of Kuwait. Several cases have been opened under Law No. 35, but only two cases have gone to court. The cases reportedly involved money smuggling and failure to report currency transactions and did not involve banks.

The National Committee for Anti-Money Laundering and the Combating of Terrorist Financing (AML/CTF) is responsible for administering Kuwait's AML/CTF regime. In April 2004, the Ministry of Finance issued Ministerial Decision No. 11 (MD No. 11/224), which transferred the chairmanship of the National Committee, formerly headed by the Minister of Finance, to the Governor of the Central Bank of Kuwait. The Committee is comprised of representatives from the Ministries of Interior, Foreign Affairs, Commerce and Industry, Finance, and Labor and Social Affairs; the Office of Public Prosecution; the Kuwait Stock Exchange; the General Customs Authority; the Union of Kuwaiti Banks; and CBK.

Since its inception, the National Committee has pursued its mandate of drawing up the country's strategy and policy with regard to anti-money laundering and terrorist financing; drafting the necessary legislation and amendments to Law No. 35, along with pertinent regulations; coordinating between the concerned ministries and agencies in matters related to combating money laundering and terrorist financing; following up on domestic, regional, and international developments and making needed recommendations in this regard; setting up appropriate channels of communication with regional and international institutions and organizations; and representing Kuwait in domestic, regional, and international meetings and conferences. In addition, the Chairman is entrusted with issuing regulations and procedures that he deems appropriate for the Committee's duties, responsibilities, and organization of its activities.

Kuwait, however, has been unable to fully implement its anti-money laundering law stipulations due in part to structural inconsistencies within the law itself, and the unwillingness of government officials to undertake the necessary steps to rectify such shortfalls. Kuwait's financial intelligence unit (FIU) is not an independent body in accordance with international standards, but rather is under the direct supervision of the Central Bank of Kuwait. In addition, vague delineation of the roles and responsibilities of the government entities involved continues to hinder the overall effectiveness of Kuwait's anti-money laundering regime. Cognizant of these shortcomings, the National Committee continues to promise to revise Law No. 35 in a manner that would bring Kuwait into compliance with international standards, and would criminalize terrorist financing.

In addition to Law No. 35, anti-money laundering reporting requirements and other rules are contained in CBK instructions No. (2/sb/92/2002), which took effect on December 1, 2002, superseding instructions No. (2/sb/50/97). The revised instructions provide for, inter alia, customer identification and the prohibition of anonymous or fictitious accounts (Articles 1-5); the requirement to keep records of all banking transactions for five years (Article 7); electronic transactions (Article 8); the requirement to investigate transactions that are unusually large or have no apparent economic or lawful purpose (Article 10); the requirement to establish internal controls and policies to combat money laundering and terrorist financing, including the establishment of internal units to oversee compliance with relevant regulations (Article 14 and 15); and the requirement to report to the CBK all cash transactions in excess of the equivalent of $10,000 (Article 20). In addition, the CBK distributed detailed instructions and guidelines to help bank employees identify suspicious transactions. At the Central Bank's instructions, in an effort to avoid "tipping off" suspected accountholders, banks are no longer required to block assets for 48 hours on suspected accounts. The Central Bank, upon notification from the Ministry of Foreign Affairs (MFA), issues circulars to units subject to supervision requiring them to freeze the assets of suspected terrorists and terrorist organizations listed on the UNSCR 1267 Sanctions Committee's consolidated list. Financial entities are instructed to freeze any such assets immediately and for an indefinite period of time, pending further instructions from the Central Bank, which in turn receives its designation guidance from the MFA.

On June 23, 2003, the CBK issued Resolution No. 1/191/2003, establishing the Kuwaiti Financial Inquiries Unit as the FIU within the Central Bank. The FIU is comprised of seven part-time Central Bank officials and headed by the Central Bank Governor. Among its responsibilities, the FIU is to receive and analyze reports of suspected money laundering activities from the OPP, establish a database of suspicious transactions, conduct anti-money laundering training, and carry out domestic and international exchanges of information in cooperation with the OPP. Law No. 35/2002 did not mandate the FIU to act as the central or sole unit for the receipt, analysis, and dissemination of STRs; instead, these functions were divided between the FIU and OPP.

Banks in Kuwait are required to file STRs with the OPP, rather than directly with the FIU. However, based on a memorandum of understanding with the Central Bank, STRs are referred from the OPP to the FIU for analysis. The FIU conducts analysis and reports any findings to the OPP for the initiation of a criminal case, if necessary. The FIU's access to information is limited, due to its inability to share

information abroad without prior approval from the OPP. Kuwaiti officials agree that the current limits on information sharing by the FIU will be addressed by draft amendments to the law, which was revised by the National Committee in 2006 and is currently under governmental review.

There are about 148 money exchange businesses (MEBs) operating in Kuwait that are authorized to exchange foreign currency only. MEBs are not formal financial institutions, so they fall under the supervision of the Ministry of Commerce and Industry (MOCI) rather than the Central Bank. The CBK has reached an agreement that tasks the MOCI with the enforcement of all anti-money laundering (AML) laws and regulations in supervising such businesses. This agreement also stipulates that the MOCI must encourage MEBs to apply for and obtain company licenses, and to register with the CBK.

The MOCI's Office of Combating Money Laundering Operations was established in 2003 and supervises approximately 2,500 insurance agents, brokers and companies; investment companies; exchange bureaus; jewelry establishments (including gold, metal and other precious commodity traders); brokers in the Kuwait Stock Exchange; and other financial brokers. All new companies seeking a business license are required to receive AML awareness training from the MOCI before a license is granted. These firms must abide by all regulations concerning customer identification, record keeping of all transactions for five years, establishment of internal control systems, and the reporting of suspicious transactions. MOCI conducts both mandatory follow-up visits and unannounced inspections to ensure continued compliance. The Office of Combating Money Laundering Operations is also actively engaged in a public awareness campaign to increase understanding about the dangers of money laundering.

Businesses found to be in violation of the provisions of Law No. 35/2002 receive an official warning from MOCI for the first offense. The second and third violations result in closure for two weeks and one month respectively. The fourth violation results in revocation of the license and closure of the business. Reportedly, four exchange houses were closed in 2006 for violating MOCI's instructions, and one case was referred to the Public Prosecutor's Office for violation of customer contracts.

In August 2002, the Kuwaiti Ministry of Social Affairs and Labor (MOSAL) issued a ministerial decree creating the Department of Charitable Organizations (DCO). The primary responsibilities of the department are to receive applications for registration from charitable organizations, monitor their operations, and establish a new accounting system to ensure that such organizations comply with the law both at home and abroad. The DCO has established guidelines for charities explaining donation collection procedures and regulating financial activities. The DCO is also charged with conducting periodic inspections to ensure that charities maintain administrative, accounting, and organizational standards in accordance with Kuwaiti law. The DCO mandates the certification of charities' financial activities by external auditors and limits the ability to transfer funds abroad only to select charities approved by MOSAL. MOSAL also requires all transfers of funds abroad to be made between authorized charity officials. Banks and money exchange businesses (MEBs) are not allowed to transfer any charitable funds outside of Kuwait without prior permission from MOSAL. In addition, any such wire transactions must be reported to the CBK, which maintains a database of all transactions conducted by charities. Unauthorized public donations, including Zakat (alms) collections in mosques, are also prohibited.

In 2005, MOSAL introduced a pilot program requiring charities to raise donations through the sale of government-provided coupons during the Muslim holy month of Ramadan. MOSAL continued this program and in 2007 implemented collection of donations through a voucher system and electronic bank transfers. Plans are underway to further encourage the electronic collection of funds using a combination of electronic kiosks, hand-held collection machines, and text messaging. These devices will generate an electronic record of the funds collected, which will then be subject to MOSAL supervision.

Kuwait is a member of the Gulf Cooperation Council (GCC), which is itself a member of the Financial Action Task Force (FATF). Kuwait is also a member of the Middle East and North Africa Financial Action Task Force (MENAFATF), a FATF-style regional body that was established in November 2004. Kuwait has played an active role in the MENAFATF through its participation in the drafting of regulations and guidelines pertaining to charities oversight and cash couriers

Kuwait is a party to the 1988 UN Drug Convention. In May 2006, Kuwait ratified the UN Convention against Transnational Organized Crime. In February 2007, Kuwait ratified the UN Convention against Corruption. Kuwait has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Kuwait should significantly accelerate its ongoing efforts to revise Law No. 35/2002 to criminalize terrorist financing; strengthen charity oversight, especially in overseas operations; develop an independent FIU that meets international standards including the sharing of information with foreign FIUs, as well as sharing between the government and financial institutions. Kuwait should implement and enforce a uniform cash declaration policy for inbound and outbound travelers. Kuwait, like many other countries in the Gulf, relies on STRs to initiate money laundering investigations. As a result, there are few investigations or prosecutions. Instead, Kuwaiti law enforcement and customs authorities should be proactive in identifying suspect behavior that could be indicative of money laundering and/or terrorist financing, such as the use of underground financial systems. Kuwait should become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

## Laos

Laos is neither an important regional financial center, nor an offshore financial center. Although the extent of the money laundering risks are unknown, illegal timber sales, corruption, cross-border smuggling of goods, illicit proceeds from the sale of methamphetamine (ATS) known locally as “ya ba” (crazy medicine), and domestic crime can be sources of laundered funds. There are continued reports of illicit funds being diverted into some hotel construction, resort development, and industrial tree cropping projects. Anecdotal evidence indicates that large cash deposits related to illicit activities are generally made across the border in Thailand.

The Lao banking sector is dominated by state-owned commercial banks in need of continued reform. Although some foreign banks have branches in Laos, the classic “offshore” banks are not permitted. The small scale and poor financial condition of Lao banks may make them more likely to be venues for certain kinds of illicit transactions. These banks are not optimal for moving large amounts of money in any single transaction, due to the visibility of such movements in the existing small-scale, low-tech environment. Reportedly, there has been no notable increase in financial crimes. There have been no money laundering investigations initiated to date. There is smuggling of consumer goods across the Mekong and in areas near the Chinese border in the north, which could be associated with trade-based money laundering. This smuggling activity is an easy way to avoid paying customs duties and the inconvenience of undergoing weigh station inspections near the Lao and Chinese borders. There are two special economic zones in Savannakhet Province, one each near the Thai and Vietnamese borders on the recently opened Danang-Bangkok highway. Both are awaiting tenants and there is no indication they are currently used to launder money or finance terrorism. China has leased a similar special economic zone in Luang Nam Tha Province on the China-Thailand Highway at Boten. Within the zone is a casino that potentially could be utilized to launder funds, though there is no evidence that the gaming facility is currently being employed for that purpose. All foreign investment in Laos must first be approved by the government’s Ministry of Planning and Investment, which provides due diligence on companies seeking to invest in Laos. Due to general poverty, lack of human

capacity, and weak governance, the ability to successfully discover companies bent on illicit transactions is suspect.

Money laundering is a criminal offense in Laos and covered in at least two separate decrees. The penal code contains a provision adopted in November 2005 that criminalizes money laundering and provides sentencing guidelines. On March 27, 2006, the Prime Minister's Office issued a detailed decree, No. 55/PM, on anti-money laundering, based on a model law provided by the Asian Development Bank. Because of the unique nature of Lao governance, the decree is roughly equivalent to a law and is much easier to change than a law passed by the National Assembly. However, it is unclear if the decrees have the same legal effect as provisions in the penal code. One provision of the decree criminalizes money laundering in relation to all crimes with a prison sentence of a year or more. In addition, the decree specifically criminalizes money laundering with respect to: terrorism; financing of terrorism; human trafficking and smuggling; sexual exploitation; human exportation or illegal migration; the production, sales, and possession of narcotic drugs; illicit arms and dynamite trafficking; concealment and trafficking of people's property; corruption; the receipt and giving of bribes; swindling; embezzlement; robbery; property theft; counterfeiting money and its use; murder and grievous bodily injury; illegal apprehension and detention; violation of state tax rules and regulations; extortion; as well as check forgery and the illicit use of false checks, bonds, and other financial instruments. The GOL is considering drafting an AML/CTF law to create a comprehensive AML/CTF regime in line with the international standards as set out by the FATF.

A revision to the penal law in November 2005 includes Article 58/2 which makes financing terrorism punishable by fines of 10 to 50 million Kip (approximately U.S. $10,000-$50,000,), prison sentences from 10 to 20 years, and the possibility of the death penalty. The Bank of Laos has circulated lists of individuals and entities on the UN 1267 Sanctions Committee's consolidated list.

A six-person Anti-Money Laundering Intelligence Unit (AMLIU) was formally established as an independent unit within the Bank of Laos on May 14, 2007, replacing the previous ad hoc Financial Intelligence Unit (FIU). According to the GOL report presented at the July 2007 Asia-Pacific Group plenary, the AMLIU Director and staff "have an action plan to develop full functionality of the AMLIU and to implement provisions of the Decree on Prevention of Money Laundering". The AMLIU acts as an FIU and supervises financial institutions for their compliance with anti-money laundering/counter-terrorist financing decrees and regulations. The AMLIU has no criminal investigative responsibilities, nor does it have any agreements with other FIUs. It is currently beginning a process to set up a National Coordinating Committee that will allow the AMLIU to interact with other relevant Lao governmental agencies such as the Ministry of Public Security. It does not yet have the technology to access the databases of local banks directly. The AMLIU created a five-part, 48-question suspicious transaction report (STR) form and distributed it to all banks along with guidance on October 15, 2007. While banks are required to report suspicious transactions, there have been no reports in 2007 to date, nor have there been any arrests for terrorist financing or money laundering.

The guidance issued by the AMLIU related to suspicious transactions, Bank of Lao No. 66/AMLIU, dated October 15, 2007, does not contain any thresholds for reporting STRs. Instead, it requires financial institutions to take into account a wide range of factors that could indicate an illegal transaction. However, any transaction over U.S. $10,000 is in practice considered worthy of further investigation. Reporting officers are protected against any suit or action related to the reporting process. While the 2006 decree on money laundering specifically applies to nonbank financial institutions (NBFI), the AMLIU is currently working only with commercial banks as it implements the STR form. It will expand its oversight once the necessary agreements with other supervising agencies are in place. Effective adoption of the STR system is likely to take a number of years. Cultural norms are such that it is unlikely that banks and NBFIs will soon begin generating reports related to

customers perceived as being either influential, politically powerful, or coming from prominent families.

Lao law restricts the export of the national currency, the kip, limiting residents and nonresidents to 5,000,000 kip per trip (approximately U.S. $500). Larger amounts may be approved by the Bank of Laos. It is likely that the currency restrictions and undeveloped banking sector encourage the use of alternative remittance systems. When carrying cash across international borders, Laos requires a declaration for amounts over U.S. $5,000 when brought into the country and when being taken out. Failure to show a declaration of incoming cash when exporting it could lead to seizure of the money or a fine. As customs procedures in Laos are undeveloped and open to corruption, enforcing this decree will require political will, development of a professional customs service, compensation reform, further training, and increased capital investments. The Prime Minister's decree on money laundering specifically authorizes asset seizures when connected to money laundering and related crimes. The authority is broadly worded. It is not clear which government authority has responsibility for asset seizures; although indications are that the Ministry of Justice would take the lead. The Government of Laos continues to build a framework of law and institutions; however, at this stage of development, enforcement of enacted legislation and decrees is weak. No legal asset seizures related to narcotics trafficking or terrorism was reported in 2007. A considerable number of assets are reportedly seized by police counternarcotics units from suspected drug traffickers, but these assets usually remain in the custody of the police. Laos is currently drafting a law that will allow for the selling of such seized assets, but, until such a law is passed, most of these assets remain under police custody.

Laos' decree on money laundering authorizes the government to cooperate with foreign governments to deter money laundering of any sort, with caveats for the protection of national security and sovereignty. There are no specific agreements with the United States relating to the exchange of information on money laundering. The Bank of Laos has coordinated with the Embassy on a number of cases related to counterfeit U.S. currency.

The GOL is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. The GOL participates in Association of Southeast Asian Nations (ASEAN) regional conferences on money laundering. Laos moved from observer status to membership in the Asia Pacific Anti-Money Laundering Group during the July 2007 Annual Meeting.

To comport with international standards, the Government of Laos should enact comprehensive anti-money laundering/counter-terrorist financing legislation, as decrees are not recognized by international organizations as having the force of law. Such legislation would include, but not be limited to, the promulgation of implementing regulations, the establishment of a viable financial intelligence unit, increasing the number and type of obligated entities, prohibition against "tipping-off", and safe harbor for those reporting suspicious financial transactions to the FIU. Laos should become a party to the UN International Convention for the Suppression of Financing of Terrorism and ratify the UN Convention against Corruption.

## Latvia

Latvia is a growing regional financial center that has a large number of commercial banks with a sizeable nonresident deposit base. Sources of laundered money in Latvia primarily involve tax evasion, but also include counterfeiting, corruption, white-collar crime, extortion, financial/banking crimes, stolen cars, contraband smuggling, and prostitution. Some proceeds of tax evasion appear to originate from outside of Latvia. A portion of domestically obtained criminal proceeds is thought to derive from organized crime. Reportedly, Russian organized crime is active in Latvia. State Narcotics Police have reportedly not found a significant link between smuggled goods on the black market and narcotics proceeds. Currency transactions involving international narcotics trafficking proceeds do not include significant amounts of United States currency and apparently do not derive from illegal drug

sales in the United States. However, U.S. law enforcement agencies think that there are ties between U.S criminal elements and the Latvian financial sector, that involve the establishment of U.S.-based shell companies to launder narcotics money through the Latvian financial sector. U.S. law enforcement agencies continue to cooperate with Latvian counterparts on matters of money laundering and affiliated crimes. As Latvia's banking controls tighten, regulators report a pattern of certain accounts moving to Lithuania and Estonia. Regulators assert that alleged criminal activity is moving to these two countries as easier places to conduct business. However, there is insufficient data available for United States authorities to assess this claim.

Latvia is not an offshore financial center, although four special economic zones exist in Latvia providing a variety of significant tax incentives for the manufacturing, outsourcing, logistics centers, and transshipment of goods to other free trade zones. These zones are located at the free ports of Ventspils, Riga, and Liepaja, and in the inland city of Rezekne near the Russian and Belarusian borders. Though there have been instances of reported cigarette smuggling to and from warehouses in the free trade zones, there have been no confirmed cases of the zones being used for money laundering schemes or by the financiers of terrorism. Latvia's banking regulator, the Financial and Capital Market Commission (FCMC), states that the zones are covered by the same regulatory oversight and enterprise registration regulations that exist for nonzone areas.

The Government of Latvia (GOL) criminalized money laundering for all serious crimes in 1998. Latvia's new anti-money laundering (AML) law, The Law on Prevention of Money Laundering and Terrorist Financing is before the Parliament, which is expected to enact it in 2008. Entities subject to the law include credit and financial institutions, tax advisors, external accountants, sworn auditors and lawyers, notaries, company service providers, real estate agents, and lottery and gambling organizers. This new law introduces a risk-based approach, where entities must assess the client's risk for anti-money laundering and terrorist financing, then choose between simplified and enhanced customer due diligence. The law includes compulsory identification of customers who pay cash for transactions of 15,000 euros (approximately U.S. $21,600) or more.

The law requires financial institutions to gather customer identification and institutes record keeping requirements. Financial institutions must keep transaction and identification data for at least five years after ending a business relationship with a client. Institutions engaging in financial transactions must report both suspicious activities and unusual transactions, including large cash transactions, to the financial intelligence unit (FIU). Suspicious transactions must be reported immediately. Financial institutions receive a list of indicators that, when present, activate the reporting requirement for an unusual transaction. Obliged entities must also file an unusual activity report using the indicator list as a basis if there is suspicion regarding laundering or attempted laundering of the proceeds from crime or terrorist financing.

Obliged entities must also report cash transactions. This requirement applies regardless of whether there is one large transaction or several smaller transactions equal to or exceeding 40,000 lats (approximately U.S. $80,000). The new Law on Prevention of Money Laundering and Terrorist Financing will reduce this amount to 15,000 euros (approximately U.S. $21,600) if it passes the 2008 Parliament readings without modification. Financial institutions have the ability to freeze accounts if they suspect money laundering or terrorist financing. If a financial institution finds the activity of an account questionable, it may close the account on its own initiative. Negligent money laundering is illegal in Latvia, and deliberately providing false information about a beneficial owner to a credit or financial institution is also illegal.

Additional amendments to the criminal law enhance the ability of Latvian law enforcement agencies to share information with one another and with Latvia's FCMC. Latvia's Criminal Procedures Law removes many procedural hurdles that had previously served as obstacles to law enforcement agencies aggressively investigating and prosecuting financial crimes. For example, prosecutors no longer need

to prove willful blindness of the criminal origin of funds before charging a person or institution with a financial crime.

Council of Ministers Regulation 55, which was replaced by 233, created what is now the Council for Development of the Financial Sector, a coordinator of AML and counter-terrorist financing (CTF) issues on the state level. The Prime Minister chairs this body.

Latvia underwent a joint Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL)/ International Monetary Fund (IMF) evaluation in March 2006 which assessed the country's AML regulatory and legal framework. Approved as MONEYVAL's third-round evaluation of Latvia in September 2006, MONEYVAL published the mutual evaluation report (MER) report in June 2007. On the 49 recommendations, 47 of which were applicable, Latvia received 26 ratings of at least "largely compliant," and only five ratings of "noncompliant."

Latvian legislation instituting a cross-border currency declaration requirement took effect on July 1, 2006. The law obliges all persons transporting more than 10,000 euros (approximately U.S. $14,700) in cash or monetary instruments into or out of Latvia, with the exception of into or out of other European Union (EU) member states, to declare the money to a customs officer, or, where there is no customs checkpoint, to a border guard. People moving within the EU are not required to declare. Latvian government agencies share these declarations amongst themselves.

Banks are not allowed to open accounts without conducting customer due diligence and obtaining client identification documents for both residents and nonresidents. When conducting due diligence on legal entities, banks must collect information on incorporation and registration. Sanctions against banks for noncompliance provide for fines up to 100,000 lats (approximately U.S. $200,000). Latvia does not have secrecy laws that prevent the disclosure of client and ownership information to bank supervisors or law enforcement officers. Safe harbor provisions protect reporting individuals.

The Bank of Latvia supervises the currency exchange sector. The FCMC serves as the GOL's unified public financial services regulator, overseeing commercial banks and nonbank financial institutions, the Riga Stock Exchange, and insurance companies. The FCMC conducts regular audits of credit institutions. It also applies sanctions to companies that fail to file mandatory reports of unusual transactions and to those that submit incomplete or deficient information on both the economic activities of businesses, and deficiencies in internal controls of banks. The FIU also works to ensure accurate reporting by determining if it has received corresponding suspicious transactions reports (STRs) when suspicious transactions occur between Latvian banks.

The FCMC has distributed regulations for customer identification and detecting unusual transactions, as well as regulations regarding internal control mechanisms that financial institutions should have in place. The FCMC has the authority to share information with Latvian law enforcement agencies and receive data on potential financial crime patterns uncovered by police or prosecutors. New regulations, drafted by FCMC, in accordance with the adopted Law on the Prevention of Money Laundering and Terrorist Financing should be finalized in early 2008. The Gambling and Lotteries Law states gaming and lottery organizers' rights and obligations in relation to the prevention of legalization of proceeds from criminal activities. Organizers are subject to restrictions and must submit suspicious or unusual transaction reports. They also perform other AML activities as required by Latvian law. The MONEYVAL MER found compliance with requirements of both the European Parliament Directives and the Financial Action Task Force (FATF) 40 Recommendations and Nine Special Recommendations on Terrorist Financing.

In addition to the legislative and regulatory requirements in place, the Association of Latvian Commercial Banks (ALCB) plays an active role in setting standards on AML issues for Latvian banks. The ALCB has adopted the regulations on the "Prevention of Money Laundering" as guidance, as well

as a "Declaration on Taking Aggressive Action against Money Laundering," which all Latvian banks signed. The ACLB has also adopted a voluntary measure, which all of the banks observe, to limit cash withdrawals from automated teller machines to 1,000 lats (approximately U.S. $2,000) per day. In October 2007, ALCB approved an "Action Plan to Enhance Transparency of Offshore Customers Serviced by Banks in Latvia on a Compliance Officers Level." Latvia expects to have fully implemented the action plan by July 2008. In addition to acting as an industry representative to government and the regulator, the ACLB organizes regular education courses on AML/CTF issues for bank employees. In the year and a half since the training program began, more than 110 AML/CTF professionals successfully passed a five-day extensive training program and examination. A total of 360 professionals have passed examinations for all of the offered AML/CTF training courses.

The Office for the Prevention of the Laundering of Proceeds Derived from Criminal Activity, known as the Control Service, is Latvia's FIU. Although it is part of the Latvian Prosecutor General's Office, its budget is separate. The Control Service has the overall responsibility for coordination, application and assessment of Latvia's AML policy and its effectiveness. The Control Service received approximately 27,000 reports in 2006. During the first 10 months of 2007 the Latvian FIU received 27,389 reports of suspicious and unusual financial transactions. The Control Service, between January and October, sent 126 cases, which include 1604 reports about suspicious and unusual financial transactions, to law enforcement authorities.

Latvia has taken steps to remedy the situation described by the MER, in which "The vast bulk of the suspicious transaction reports filed are based on the Cabinet of Ministers list of indicators of unusual transactions and the FIU list of indicators/examples. Only a very small minority of the reports are based on suspicions formed under other circumstances. The assessors were informed that the financial institutions follow the FIU list and automatically report transactions that meet at least one of the examples (although the indicators are only examples). This would suggest that the financial institutions may be relying too heavily on the lists provided and might not be exercising appropriate discretion on the circumstances that are not covered by the lists of indicators. This could result in overdependence on the indicators/examples results and submission to the Control Service of significant numbers of reports with little or no value for FIU analytical purposes. It was not possible for the assessors to determine whether or not financial institutions were giving sufficient attention to identifying and reporting real (as distinct from indicator-based) suspicious transactions, as there were some conflicting indications. The assessors were not provided by the Control Service with statistics separating indicator-based STRs from reports based on direct suspicion." The new draft legislation defines a suspicious transaction, but does not list indicators for determining suspicious transactions, forcing the obliged entities to themselves execute transaction analyses.

Latvia has also taken steps to ensure effective implementation of the draft law by providing training to explain the intent and issues to the law's subjects. Both individual financial institutions and entire sectors, such as tax consultants, have received this training. The ALCB organizes five-day seminars for this purpose, and certifies the attending staff. The ALCB provided two such trainings in 2007.

The Control Service conducts a preliminary investigation of the suspicious and unusual reports. It may then forward the information to law enforcement authorities that investigate money laundering cases. The Control Service can disseminate case information to a specialized Anti-Money Laundering Investigation Unit of the Economic Police within the State Police; and the Office for the Combat of Organized Crime. The FIU can also disseminate information to the Financial Police (under the State Revenue Service of the Ministry of Finance); the Bureau for the Prevention and Combat of Corruption (Anti-Corruption Bureau, KNAB) for crimes committed by public officials; the Security Police (for cases concerning terrorism and terrorist financing); and other law enforcement authorities. According to the draft law, the FIU will have to decide within 14 days of receiving a report whether there are grounds to open a case. If the FIU decides to open a case, it will have the authority to suspend the transaction for 30 days. During the 30 days, the FIU will gather information on the transaction and the

parties involved. If the FIU determines grounds for starting a criminal procedure, the FIU can further suspend the transaction for up to 45 days.

The Control Service has access to all state and municipal databases. It does not have direct access to the databases of financial institutions, but requests data as needed. The Control Service shares data with other FIUs and has cooperation agreements on information exchange with FIUs in sixteen countries. Latvia has also signed multilateral agreements with several EU countries to automatically exchange information with the EU financial intelligence units using FIU. The Control Service is a member of the Egmont Group of financial intelligence units.

In 2006, the Latvian FIU issued 125 orders to freeze assets, freezing a total of 12.6 million lats (approximately U.S. $23.5 million). During the first 10 months of 2007 the Latvian FIU issued 80 freezing orders for the total amount of U.S. $12.24 million. Latvia's FIU reports that cooperation from the banking community to trace and freeze assets has been excellent.

The adoption of Latvia's 2005 Criminal Procedures Law provides measures for the seizure and forfeiture of assets. The law enables law enforcement authorities to identify, trace, and confiscate criminal proceeds. Investigators can initiate an action for the seizure of assets recovered during a criminal investigation concurrently with the investigation itself—they do not need to wait until the investigation is complete. During the first 10 months of 2007, the courts returned 14 decisions, leading to the confiscation of approximately U.S. $2.57 million worth of assets on behalf of the state. Proceeds from asset seizures and forfeitures go into the state treasury.

The Prosecutor General's Office maintains a specialized staff to prosecute cases linked to money laundering. The seven staff prosecutors have undergone a special clearance process. In 2006, the Prosecutor General's Office received ten money laundering cases for the prosecution of 47 individuals. In three of the cases, four individuals received convictions and sentences including time in jail. During the first 10 months of 2007 the Prosecutor's Office received 11 money laundering cases for the prosecution of 40 individuals, and reviewed eight money laundering cases resulting in the sentencing of 12 people.

The GOL has initiated measures aimed at combating the financing of terrorism. Article 88-1 of the Criminal Code criminalizes terrorist financing, and meets the United Nations Security Council Resolution (UNSCR) 1373 requirements. It has issued regulations to implement the sanctions imposed by UNSCR 1267. The regulations require that financial institutions report to the Control Service, transactions related to any individual or organization on the UNSCR 1267 Sanctions Committee's consolidated list or on other terrorist lists, including those shared with Latvia by international partners. The Control Service maintains consolidated terrorist finance and watch-lists and regularly distributes these to financial and nonfinancial institutions, as well as to their supervisory bodies. On several occasions, Latvian financial institutions have temporarily frozen monetary funds associated with names on terrorist finance watch lists, including those issued by the U.S. Office of Foreign Assets Control (OFAC), although authorities have found no confirmed matches to names on the list. Article 17 of the AML law authorizes the Control Service to freeze the funds of persons included on one of the terrorist lists for up to six months. Latvia employs the same freezing mechanism with regard to terrorist assets as it uses with those relating to other crimes but includes involvement by the Latvian Security Police. Authorities handle associated investigations, asset and property seizures, in accordance with the Criminal Procedures Law.

Latvia took swift action to improve its AML/CTF regime after the United States outlined concerns in a Notices of Proposed Rulemaking against two Latvian banks on April 26, 2005, under Section 311 of the USA PATRIOT Act. According to the IMF/MONEYVAL MER, "At one point in 2005, 13 of the 23 Latvian banks were subject by the FCMC to the legal status of intensified supervision due to deficiencies in their AML/CTF systems, as the FCMC pursued strong measures to clean up the banking system." On August 14, 2006, the United States issued a final rule imposing a special

measure against one of the two banks, VEF Banka, as a financial institution of primary money laundering concern. This measure, specific to VEF Banka, is still in effect.

Latvia permits only conventional money remitters (such as Western Union and Moneygram). The remitters work through the banks and not as separate entities. Alternative remittance services are prohibited in Latvia. The Control Service has not detected any cases of charitable or nonprofit entities used as conduits for terrorist financing in Latvia

Latvia is a party to the UN International Convention for the Suppression of the Financing of Terrorism and eleven other multilateral counter-terrorism conventions. Latvia is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. A Mutual Legal Assistance Treaty (MLAT) has been in force between the United States and Latvia since 1999. Latvia is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL).

The GOL should enact additional amendments to its legislation to tighten its AML framework. It should continue to implement and make full use of the 2005 amendments to its Criminal Procedures Law and upon enactment, actively implement and vigorously enforce the new AML law. Supervisory authorities should draft necessary implementing regulations in advance and perform outreach so that upon enactment of the legislation, the obliged entities will be able to comport with the law's requirements. Latvia needs to strengthen its risk-based approach to AML/CTF and take steps to further enhance the preventative aspects of its AML/CTF regime, including improved customer due diligence requirements and increased scrutiny of higher risk categories of transactions, clients and countries. The GOL should continue to take steps to increase information sharing and cooperation between law enforcement agencies at the working level. The GOL should also strengthen its ability to aggressively prosecute and convict those involved in financial crimes.

## Lebanon

Lebanon is a financial hub for banking activities in the Middle East and eastern Mediterranean. It has one of the more sophisticated banking sectors in the region. The banking sector continues to record an increase in deposits. As of October 2007, there were 65 banks (51 commercial banks, 11 investment banks, and three Islamic banks) operating in Lebanon with total deposits of U.S. $70 billion. One U.S. bank (Citibank) and four U.S bank representative offices operate in Lebanon: American Express Bank, the Bank of New York, JP Morgan Chase Bank National Association, and Morgan Guarantee Trust Co. of New York.

The Central Bank of Lebanon, Banque du Liban, regulates all financial institutions and money exchange houses. Lebanon imposes no controls on the movement of capital. It has a substantial influx of remittances from expatriate workers and family members, estimated by banking sources to reach U.S. $4 to 5 billion yearly. Such family ties are reportedly involved in underground finance and trade-based money laundering.

Laundered criminal proceeds come primarily from domestic criminal activity, which is largely controlled by organized crime. In May 2007, members of the terrorist group Fatah Al-Islam stole $150,000 from a BankMed branch in Tripoli in northern Lebanon. There is some smuggling of cigarettes and pirated software, but this does not generate large amounts of funds that are laundered through the banking system. There is a black market for counterfeit goods and pirated software, CDs, and DVDs. Lebanese customs officials have had some recent success in combating counterfeit and pirated goods. The illicit narcotics trade is not a principal source of money laundering proceeds.

Offshore banking, trust and insurance companies are not permitted in Lebanon. Legislative Decree No. 46 of 1983 restricts offshore companies' activity to negotiating and signing advisory and services agreements, in addition to sale and purchase contracts of products and goods, all concerning business

conducted outside of Lebanon or in the Lebanese Customs Free Zone. Thus, offshore companies are barred from engaging in activities such as industry, banking, and insurance. All offshore companies must register with the Beirut Commercial Registrar, and the owners of an offshore company must submit a copy of their identification. Moreover, the Beirut Commercial Registrar keeps a special register, in which all information about the offshore company is retained. A draft law amending legislation on offshore companies to comply with World Trade Organization's standards was still pending in Parliament as of early November 2007.

There are currently two free trade zones operating in Lebanon, at the Ports of Beirut and Tripoli. The free trade zones fall under the supervision of Customs. Exporters moving goods into and out of the free zones submit a detailed manifest to Customs. Customs is expected to report suspected trade-based money laundering or terrorist financing to the Special Investigation Commission (SIC), Lebanon's financial intelligence unit (FIU). Companies using the free trade zone must be registered and must submit appropriate documentation, which is kept on file for a minimum of five years. Lebanon has no cross-border currency reporting requirements. However, since January 2003, Customs checks travelers randomly and notifies the SIC upon discovery of large amounts of cash.

In 2004, Lebanon passed a law requiring diamond traders to seek proper certification of origin for imported diamonds; the Ministry of Economy and Trade (MOET) is in charge of issuing certification for re-exported diamonds. This law was designed to prevent the trafficking of "conflict diamonds" and allowed Lebanon to participate in the Kimberley Process in September 2005. Prior to this, Lebanon passed a decree in August 2003 prohibiting imports of rough diamonds from countries that are participants in the Kimberley Process. There have been consistent reports that some Lebanese diamond brokers in Africa are engaged in the laundering of diamonds—the most condensed form of physical wealth in the world. However, the Kimberley Process office in Lebanon stressed that importers or exporters of rough diamonds must submit an application to MOET to import or export rough diamonds according to the Kimberley Process procedure. The Beirut International Airport is the sole entry point for rough diamonds. The Kimberley Process office at the Beirut International Airport monitors and physically checks the quantities of rough diamonds imported, making sure that imports carry a Kimberley Process certification issued by the country of origin. It also checks on exports of rough diamonds from Lebanon to other member countries of the Kimberley Process. In 2007, Customs had two cases where they seized smuggled rough diamonds that were not carrying the Kimberley certification. Customs kept the rough diamonds in custody and notified the Kimberley Process office at MOET. The Kimberley Process Committee referred the two cases to the State Prosecutor, and both cases are now in the Lebanese court. Yet these safeguards do not address the issue of smuggled diamonds, the purchase of fraudulently obtained Kimberley Process certificates, the laundering of diamonds, or value transfer via the diamond trade.

Lebanon has a large expatriate community throughout the Middle East, Africa, and parts of Latin America. They often work as brokers and traders. Many Lebanese "import-export" concerns are found in free trade zones. Some of these Lebanese brokers network via family ties and are involved with underground finance and trade-based money laundering. Informal remittances and value transfer in the form of trade goods add substantially to the remittance flows from expatriates via official banking channels. For example, expatriate Lebanese brokers are actively involved in the trade of counterfeit goods in the tri-border region of South America and the smuggling and laundering of diamonds in Africa. There are also reports that many in the Lebanese expatriate business community willingly or unwillingly give "charitable donations" to representatives of Hizballah (which is based in Lebanon). The funds are then repatriated or laundered back to Lebanon.

Lebanon has continued to make progress toward developing an effective money laundering and terrorist financing regime by incorporating the Financial Action Task Force (FATF) Recommendations. Lebanon enacted Law No. 318 in 2001. Law No. 318 created a framework for lifting bank secrecy, broadening the criminalization of money laundering beyond drugs, mandating

suspicious transaction reporting, requiring financial institutions to obtain customer identification information, and facilitating access to banking information and records by judicial authorities. Under this law, money laundering is a criminal offense and punishable by imprisonment for a period of three to seven years and by a fine of no less than 20 million Lebanese pounds (approximately $13,270). The provisions of Law No. 318 expand the type of financial institutions subject to the provisions of the Banking Secrecy Law of 1956, to include institutions such as exchange offices, financial intermediation companies, leasing companies, mutual funds, insurance companies, companies promoting and selling real estate and construction, and dealers in high-value commodities. In addition, Law No. 318 requires companies engaged in transactions for high-value items (i.e., precious metals, antiquities) and real estate to also report suspicious transactions.

These companies are also required to ascertain, through official documents, the identity and address of each client and must keep photocopies of these documents as well as photocopies of the operation-related documents for a period of no less than five years. The Central Bank regulates private couriers who transport currency. Western Union and Money Gram are licensed by the Central Bank and are subject to the provisions of this law. Charitable and nonprofit organizations must be registered with the Ministry of Interior and are required to have proper corporate governance, including audited financial statements. These organizations are also subject to the same suspicious reporting requirements.

All financial institutions and money exchange houses are regulated by Law No. 318 which clarifies the Central Bank's powers to: require financial institutions to identify all clients, including transient clients; maintain records of customer identification information; request information about the beneficial owners of accounts; conduct internal audits; and exercise due diligence in conducting transactions for clients.

Law No. 318 also established the Special Investigation Commission (SIC), Lebanon's FIU. SIC is an independent entity with judicial status that can investigate money laundering operations and monitor compliance of banks and other financial institutions with the provisions of Law No. 318. The SIC serves as the key element of Lebanon's anti-money laundering regime and has been the critical driving force behind the implementation process. The SIC is responsible for receiving and investigating reports of suspicious transactions. The SIC is the only entity with the authority to lift bank secrecy for administrative and judicial agencies, and it is the administrative body through which foreign FIU requests for assistance are processed

Since its inception, the SIC has been active in providing support to international criminal case referrals. From January through October 2007, the SIC investigated 182 cases involving allegations of money laundering, terrorism, and terrorist financing activities. Two of the 182 cases were related to terrorist financing. Bank secrecy regulations were lifted in 41 instances. Four cases were transmitted by the SIC to the general state prosecutor for further investigation. As of November 2007, no cases were transmitted by the general state prosecutor to the penal judge. The general state prosecutor reported seven cases to the SIC. Four cases were related to embezzlement and counterfeiting charges, one case to fraud, another to terrorism, and the last one to Interpol intelligence. From January to October 2007, the SIC froze the accounts of three individuals totaling approximately $50,000 in three of the 182 cases investigated.

During 2003, Lebanon adopted additional measures to strengthen efforts to combat money laundering and terrorist financing, such as establishing anti-money laundering units in customs and the police. In 2003, Lebanon joined the Egmont Group of financial intelligence units. The SIC has reported increased inter-agency cooperation with other Lebanese law enforcement units, such as Customs and Police, as well as with the office of the general state prosecutor. In 2005, a SIC Remote Access Communication system was put in place for the exchange of information between the SIC, Customs, the Internal Security Forces (ISF) anti-money laundering and terrorist financing unit, and the general

state prosecutor. The cooperation led to an increase in the number of suspicious transactions reports (STRs), and, as a result, the SIC initiated several investigations in 2007.

To more effectively combat money laundering and terrorist financing, Lebanon also adopted two laws in 2003: Laws 547 and 553. Law 547 expanded Article One of Law No. 318, criminalizing any funds resulting from the financing or contribution to the financing of terrorism or terrorist acts or organizations, based on the definition of terrorism as it appears in the Lebanese Penal Code. Law 547 also criminalized acts of theft or embezzlement of public or private funds, as well as the appropriation of such funds by fraudulent means, counterfeiting, or breach of trust by banks and financial institutions for such acts that fall within the scope of their activities. It also criminalized counterfeiting of money, credit cards, debit cards, and charge cards, or any official document or commercial paper, including checks. Law 553 added an article to the Penal Code (Article 316) on terrorist financing, which stipulates that any person who voluntarily, either directly or indirectly, finances or contributes to terrorist organizations or terrorists acts is punishable by imprisonment with hard labor for a period not less than three years and not more than seven years, as well as a fine not less than the amount contributed but not exceeding three times that amount.

Lebanese law allows for property forfeiture in civil as well as criminal proceedings. The Government of Lebanon (GOL) enforces existing drug-related asset seizure and forfeiture laws. Current law provides for the confiscation of assets the court determines to be related to or proceeding from money laundering or terrorist financing. In addition, vehicles used to transport narcotics can be seized. Legitimate businesses established from illegal proceeds after passage of Law 318 are also subject to seizure. Forfeitures are transferred to the Lebanese Treasury. In cases where proceeds are owed to a foreign government, the GOL returns the proceeds to the concerned government. In February 2007, two persons were convicted for laundering money.

Lebanon was one of the founding members of the Middle East and North Africa Financial Action Task Force (MENAFATF) and assumed its presidency through 2005. There is no information available on Lebanon's mutual evaluation by MENAFATF.

The SIC circulates to all financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee's consolidated list, the list of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O. 13224 and those that European Union have designated under their relevant authorities. As of early November 2007, SIC signed seventeen memoranda of understanding with counterpart FIUs concerning international cooperation.

In September 2007 the Lebanese Cabinet established a national committee that is chaired by the Ministry of Interior to suppress the financing of terrorism. The Cabinet also expanded membership of The National Committee for coordinating AML policies to include representatives from five Ministries: Justice, Finance, Interior, Foreign Affairs, and Economy, in addition to a representative from Beirut Stock Exchange. Yet prosecutions and convictions are still lacking. The end of the Syrian military occupation in April 2005 and the gradual decline of Syrian influence over the economy (both licit and illicit), security services, and political life in Lebanon may present an opportunity for the GOL to further strengthen its efforts against money laundering, corruption, and terrorist financing.

Lebanon is a party to the 1988 UN Drug Convention, although it has expressed reservations to several sections relating to bank secrecy. It has signed and ratified the UN Convention against Transnational Organized Crime. Lebanon is not a party to the UN Convention against Corruption or the UN International Convention for the Suppression of the Financing of Terrorism.

The GOL should encourage more efficient cooperation between financial investigators and other concerned parties, such as police and customs, which could yield significant improvements in initiating and conducting investigations The GOL should become a party to the UN Convention against Corruption and the UN International Convention for the Suppression of Terrorist Financing.

Per FATF Special Recommendation Nine on bulk cash smuggling, the GOL should mandate and enforce cross-border currency reporting. Lebanese law enforcement authorities should examine domestic ties to the international network of Lebanese brokers and traders that are commonly found in underground finance, trade fraud, and trade-based money laundering..

## Liechtenstein

The Principality of Liechtenstein has a well-developed offshore financial services sector, liberal incorporation and corporate governance rules, relatively low tax rates, and a tradition of strict bank secrecy. All of these conditions have contributed significantly to the ability of financial intermediaries in Liechtenstein to attract funds from abroad. These same conditions have historically made the country attractive to money launderers using the system to launder their proceeds from fraud. Although accusations of misuse of Liechtenstein's banking system persist, the principality has made substantial progress in its efforts against money laundering in recent years.

Liechtenstein's financial services sector includes 16 banks, three nonbank financial companies, 16 public investment companies, and a number of insurance and reinsurance companies. The three largest banks control ninety percent of the market. Liechtenstein's 230 licensed fiduciary companies and 60 lawyers serve as nominees for or manage more than 75,000 entities (mostly corporations or trusts) available primarily to nonresidents of Liechtenstein. Approximately one third of these entities hold controlling interests in separate entities chartered outside of Liechtenstein. Laws permit corporations to issue bearer shares.

Narcotics-related money laundering has been a criminal offense in Liechtenstein since 1993, and the number of predicate offenses for money laundering has increased over time. The Government of Liechtenstein (GOL) is reviewing the Criminal Code to further expand the list of predicate offenses. Article 165 criminalizes laundering one's own funds and imposes penalties for money laundering.

Liechtenstein enacted its first general anti-money laundering (AML) legislation in 1996. Although this law applied some money laundering controls to financial institutions and intermediaries operating in Liechtenstein, the AML regime at that time suffered from serious systemic problems and deficiencies. In response to international pressure, beginning in 2000, the GOL took legislative and administrative steps to improve its AML regime.

Liechtenstein's primary piece of AML legislation, the Due Diligence Act (DDA), applies to banks, e-money institutions, casinos, dealers in high-value goods, and a number of other entities. Along with the Due Diligence Ordinance, the DDA sets out the basic requirements of the AML regime in accordance with the Financial Action Task Force (FATF) 40 Recommendations and Nine Special Recommendations on Terrorist Financing in the areas of customer identification, suspicious transaction reporting, and record keeping. The DDA prohibits banks and postal institutions from engaging in business relationships with shell banks and from maintaining bearer-payable passbooks, accounts, and deposits. Legislation does not, however, address negligent money laundering. The suspicious-transaction reporting requirement applies to banks, insurers, financial advisers, postal services, exchange offices, attorneys, financial regulators, casinos, and other entities. The GOL has reformed its suspicious transaction reporting system to permit reporting for a much broader range of offenses than in the past. The reporting requirement now uses the basis of a suspicion, rather than the previous standard of "a strong suspicion."

The GOL announced in August 2007, that it would implement legislation enacting EU regulations requiring that money transfers above 15,000 euros (U.S. $17,678) include information on the identity of the sender, including his or her name, address, and account number. The proposed measures, to take effect by early 2008, will ensure that this information will be immediately available to appropriate law

enforcement authorities. The information will assist them in detecting, investigating, and prosecuting money launderers, terrorist financiers, and other criminals.

The Financial Market Authority (FMA) serves as Liechtenstein's central financial supervisory authority. FMA has assumed the responsibilities of several former administrative bodies, including the Financial Supervisory Authority and the Due Diligence Unit, both of which once exercised responsibility over money laundering issues. FMA reports exclusively to the Liechtenstein Parliament, making it independent from Liechtenstein's government. The FMA supervises a large variety of financial actors, including banks, finance companies, insurance companies, currency exchange offices, and real estate brokers. FMA works closely with Liechtenstein's financial intelligence unit (FIU), the Office of the Prosecutor, and the police.

Liechtenstein's FIU, known as the Einheit fuer Finanzinformationen (EFFI), receives, analyzes and disseminates suspicious transaction reports (STRs) relating to money laundering and terrorist financing. The EFFI became operational in March 2001. The EFFI has its own database as well as access to various governmental databases. However, EFFI cannot seek additional financial information unrelated to a filed suspicious transaction reports (STR.)

In 2006, the FIU received 163 STRs. Of the total of 163 STRs, banks submitted 84, professional trustees submitted 65, lawyers submitted nine, and investment companies and the Postal Service submitted one apiece. Three STRs were submitted by Liechtenstein authorities or the FMA. U.S. nationals identified as subjects of STRs comprised four percent. In 2006, the FIU received 139 inquiries from 21 different FIUs and sent 158 inquiries to 23 different FIUs. Information regarding the number of STRs received in 2007 is not yet available.

STRs have generated several successful money laundering investigations. EFFI works closely with the prosecutor's office and law enforcement authorities, in particular with a special economic and organized crime unit of the National Police known as EWOK. Police can use special investigative measures when authorized to do so by a Special Investigative Judge.

Liechtenstein has legislation to seize, freeze, and share forfeited assets with cooperating countries. The Special Law on Mutual Assistance in International Criminal Matters gives priority to international agreements. Money laundering is an extraditable offense, and Liechtenstein grants legal assistance on the basis of dual criminality. Article 235A provides for the sharing of confiscated assets. Liechtenstein has not adopted the EU-driven policy of reversing the burden of proof (i.e., forcing a defendant to prove assets were legally obtained instead of the state being required to prove their illicit nature.)

A series of amendments to Liechtenstein laws, along with amendments to the Criminal Code and the Code of Criminal Procedure, criminalize terrorist financing. Liechtenstein has implemented United Nations Security Council Resolutions (UNSCRs) 1267 and 1333. The GOL can freeze the accounts of individuals and entities that are designated pursuant to these UNSCRs. The GOL updates its implementing ordinances regularly.

The GOL has improved its international cooperation provisions in both administrative and judicial matters. A mutual legal assistance treaty (MLAT) between Liechtenstein and the United States entered into force on August 1, 2003. The U. S. Department of Justice has acknowledged Liechtenstein's cooperation in the Al-Taqwa Bank case and in other fraud and narcotics cases. The FIU has in place memoranda of understanding (MOUs) with nine FIUs, and seven others are under negotiation.

Liechtenstein is a member of the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), which discussed the most recent Liechtenstein assessment at its September 2007 plenary. However, the report is not yet available. EFFI is a member of the Egmont Group. The GOL is a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and the UN International Convention for the Suppression of the Financing of Terrorism. On March 9, 2007, Liechtenstein acceded to the

1988 UN Drug Convention. Liechtenstein has also signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. Liechtenstein has endorsed the Basel Committee's "Core Principles for Effective Banking Supervision" and has adopted the EU Convention on the Suppression of Terrorism.

The Government of Liechtenstein has made consistent progress in addressing the shortcomings in its AML regime. It should continue to build upon the foundation of its evolving anti-money laundering and counter-terrorist financing regime. Liechtenstein should ratify the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. Liechtenstein should enact and implement legislation requiring the reporting of cross-border currency movements and ensure that trustees and other fiduciaries comply fully with all aspects of AML legislation and attendant regulations, including the obligation to report suspicious transactions. The GOL should prohibit the issuance and use of corporate bearer shares. The FIU should have access to additional financial information. While Liechtenstein recognizes the rights of third parties and protects uninvolved parties in matters of confiscation, the government should distinguish between bona fide third parties and others. Liechtenstein should consider discarding its list of predicate offenses in favor of an all-crimes approach.

## Luxembourg

Despite its standing as the second-smallest member of the European Union (EU), Luxembourg is one of the largest financial centers in the world. While Luxembourg is not a major hub for illicit narcotics distribution, the size and sophistication of its financial sector create opportunities for money laundering, tax evasion, and other financial crimes. Luxembourg is an offshore financial center. Although there are a handful of domestic banks operating in the country, the majority of banks registered in Luxembourg are foreign subsidiaries of banks in Germany, Belgium, France, Italy, and Switzerland. A significant share of Luxembourg's suspicious transaction reports (STRs) are generated from transactions involving clients in these countries.

Luxembourg's strict bank secrecy laws allow international financial institutions to benefit from and operate a wide range of services and activities. With over U.S. $3.1 trillion in domiciled assets, Luxembourg is the second largest mutual fund investment center in the world, after the United States. As of October 2007, 157 registered banks existed, with a collective balance sheet total reaching approximately U.S. $1.38 trillion. In addition, as of January 2007, a total of 2,238 "undertakings for collective investment" (UCIs), or mutual fund companies, whose net assets had reached over approximately U.S. $2.66 trillion operated from Luxembourg or traded on the Luxembourg stock exchange. Luxembourg has approximately 15,000 holding companies, 95 insurance companies, and 260 reinsurance companies. In January 2006, the Luxembourg Stock Exchange listed over 39,000 securities issued by nearly 4,100 entities from 105 countries. Luxembourg also has 116 registered venture capital funds (Societe d'investissement en capital a risqué, or "SICAR").

The Law of July 7, 1989, updated in 1998 and 2004, serves as Luxembourg's primary anti-money laundering (AML) and counter-terrorist financing (CTF) law, criminalizing the laundering of proceeds for an extensive list of predicate offenses, including narcotics trafficking. The laws implement the EU's money laundering directives and provide customer identification, recordkeeping, and suspicious transaction reporting requirements. Corruption, weapons offenses, fraud committed against the EU and organized crime are on Luxembourg's list of predicate offenses for money laundering. The entities subject to money laundering regulations include banks, pension funds, insurance brokers, UCIs, management companies, external auditors, accountants, notaries, lawyers, casinos, gaming establishments, real estate agents, tax and economic advisors, domiciliary agents, insurance providers, and dealers in high-value goods such as jewelry and vehicles All obliged entities are required to file STRs with the financial intelligence unit (FIU). The current AML law does not cover SICAR entities.

The law also imposes strict "know your customer" (KYC) requirements on obliged entities for all customers, including beneficial owners, trading in goods worth at least 15,000 euros (U.S. $21,900). If the transaction or business relationship is remotely based, the law details measures required for customer identification. Entities must proactively monitor their customers for potential risk. Luxembourg's laws also prohibit "tipping off". Financial institutions must also ensure adequate internal organization and employee training, and must cooperate with authorities, The banking community generally cooperates with enforcement efforts to trace funds and seize or freeze bank accounts.

Although Luxembourg is well known for its strict banking secrecy laws, banking secrecy laws do not apply in investigations and prosecutions of money laundering and other criminal cases. A court order is not necessary for the competent authorities to investigate account information in suspected money laundering cases or in response to an STR. Financial professionals have a legal obligation to cooperate with the public prosecutor in investigating such cases. To obtain a conviction for money laundering, prosecutors must prove criminal intent rather than negligence. Negligence, however, is subject to scrutiny by competent authority, with sanctions for noncompliance varying from 1,250 to 1,250,000 euros (U.S. $1,825 to $1,825,000) and, potentially, forfeiture of the professional license. Luxembourg's regulatory authorities believe these fines to be stiff enough so as to encourage strict compliance.

On November 9, 2007, the Council of Government approved Bill 5811 to implement the Third EU Money Laundering directive. However, by year's end, the bill had not gone to the full chamber for deliberation.

At the close of 2007, Parliament was considering Bill 5756, which would bring Luxembourg into conformity with the first recommendation of the Financial Action Task Force (FATF) 40 Recommendations and Nine Special Recommendations. This recommendation encourages countries to criminalize money laundering and "apply the crime of money laundering to all serious offenses, with a view to including the widest range of predicate offenses." Bill 5756, when enacted, will widen the scope of predicate offenses in Luxembourg law and set forth minimum sentence guidelines for money laundering offenses to comport with the FATF recommendations. This bill was introduced into Parliament in August 2007, but was not scheduled for a vote at the end of 2007.

The Financial Supervision Commission (Commission de Surveillance du Secteur Financier or CSSF) is an independent body under the Ministry of Finance that acts as the supervisory authority for banks, credit institutions, the securities market, some pension funds, financial sector professionals, and other financial sector entities covered by the country's AML/CTF laws. Banks must undergo audits under CSSF supervision. All entities involved in oversight functions, including registered independent auditors, in-house bank auditors, and the CSSF, can obtain the identities of the beneficial owners of accounts. The CSSF establishes the standards for and grants "financial sector professional" ("professionnel du secteur fiancier," or PSF) status to financial sector entities. Originally covering only individual financial sector professionals having access to customer information subject to bank secrecy laws, the CSSF recently established a sub-category for service providers with potential access to that information, such as transaction-clearing houses, information technology consultants, and data warehousing services. With this status, banks have the flexibility to outsource some services while guaranteeing continued compliance with banking secrecy laws to their customers. The CSSF regulates the PSF status tightly, frequently issuing circulars and updating accreditation requirements. Accordingly, the PSF holds coveted status in the Luxembourg financial community.

The Luxembourg Central Bank oversees the payment and securities settlement system, and the Insurance Commissioner's Office (Commissariat aux Assurances or CAA), also under the Ministry of Finance, is the regulatory authority for the insurance sector.

Under the direction of the Ministry of the Treasury, the CSSF has established a committee, the Anti-Money Laundering Steering Committee (Comite de Pilotage Anti-Blanchiment or COPILAB), composed of supervisory and law enforcement authorities, the financial intelligence unit (FIU), and financial industry representatives. The committee meets monthly to develop a common public-private approach to strengthen Luxembourg's AML regime.

Luxembourg's laws and regulations do not distinguish between onshore and offshore activities. Foreign institutions seeking establishment in Luxembourg must demonstrate prior establishment in a foreign country and meet stringent minimum capital requirements. Nominee (anonymous) directors are not permitted. Companies must maintain a registered office in Luxembourg, and authorities perform background checks on all applicants. A government registry publicly lists company directors.

Luxembourg permits bearer shares. Officials contend that bearer shares do not pose a money laundering concern because of KYC laws that require banks to know the identities of beneficial owners. Banks must undergo annual audits under CSSF supervision.

Luxembourg's FIU, (Cellule de Renseignement Financier), is part of the State Prosecutor's Office and housed within Luxembourg's Ministry of Justice. The FIU consists of three State Prosecutors and one analyst. The FIU State Prosecutors pursue economic and financial crimes in Luxembourg, and spend significant portions of their time preparing for cases involving financial crimes. They are also occasionally called upon to prosecute cases not involving financial crimes.

The FIU receives and analyzes the STRs from all obliged entities. The FIU provides members of the financial community with access to updated information on money laundering and terrorist financing practices. The FIU issues circulars to all financial sector-related professionals who are not regulated under the CSSF as well as notifies the financial sector about terrorist financing designations promulgated by the EU and United Nations (UN).

By late November 2007, obliged institutions filed a total of 679 STRs, compared to a total of 754 in 2006. The number of individuals referenced in STRs has decreased dramatically from 2,471 in 2004 to 1,452 in 2006, which the FIU attributes to increased financial sector confidence in KYC practices. Among the individuals referenced in STRs in 2006, 28 resided in the United States. Of 255 confirmed cases of suspicious activity in 2006, 34 related to organized crime (including terrorist financing), 14 to narcotics-related money laundering, and 24 were related to corruption.

The FIU works with the AML Unit of the Judicial Police. Luxembourg prosecuted three money laundering cases in 2006 and four in 2007. Three were of particular note: In May 2006, two individuals were convicted of laundering narcotics-trafficking proceeds and received sentences of 72 months and 12 months of imprisonment respectively. In November 2006, five individuals were acquitted of money laundering charges when the court found that the State had not sufficiently established the linkage between the funds and either narcotics trafficking or an organized crime enterprise. The government seeks to close this legal vulnerability with Bill 5756, which expands the list of predicate offenses. Also in November 2006, a Dutch lawyer for a convicted drug trafficker was acquitted of attempted money laundering charges in November 2006, but an appellate court overturned the acquittal in May 2007. The defendant appealed his conviction to Luxembourg's Supreme Court, which should reach a judgment in 2008.

Luxembourg law only allows for criminal forfeitures and public takings. Narcotics related proceeds are pooled in a special fund to invest in anti-drug abuse programs. Luxembourg can confiscate funds found to be the result of money laundering even if they are not the proceeds of a crime. The Government of Luxembourg (GOL) can, on a case-by-case basis, freeze and seize assets, including assets belonging to legitimate businesses used for money laundering. The FIU freezes assets and issues blocking orders when necessary. The government has adequate police powers and resources to trace, seize, and freeze assets without undue delay. Luxembourg has independently frozen several

accounts. This has resulted in court challenges by the account holders, after which nearly all of the assets were subsequently released. Luxembourg has a comprehensive system not only for the seizure and forfeiture of criminal assets, but also for the sharing of those assets with other governments. Bill 5019, of August 2007, allows Luxembourg to seize assets on the basis of a foreign criminal conviction, even when there is no specific treaty in place with that country.

The Ministry of Justice studies and reports on potential abuses of charitable and nonprofit entities. Justice and Home Affairs ministers from Luxembourg and other EU member states agreed in early December 2005, to take into account five principles with regard to implementing FATF Special Recommendation VIII on nonprofit organizations: safeguarding the integrity of the sector; dialogue with stakeholders; continuing knowledge development of the sector; transparency, accountability and good governance; and effective, proportional oversight.

Luxembourg's authorities have not found evidence of the widespread use of alternative remittance systems or trade-based money laundering. Luxembourg government officials maintain that because AML rules would apply to such systems, they are not considering separate legislative or regulatory initiatives to address them.

The GOL actively disseminates to its financial institutions information concerning suspected individuals and entities on the United Nations Security Council Resolution 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to Executive Order 13224. Luxembourg's authorities can and do take action against groups targeted through the EU designation process and the UN. Luxembourg does not have legal authority to independently designate terrorist groups or individuals. The government has been working on legislation with regard to this issue for more than three years, but the legislation remains in the drafting process. Government prosecutors are confident that they could use existing judicial authority if any institution were to identify a terrorist financier. Although bilateral freeze requests have a limit of three months, designations under the EU, UN, or international investigation processes continue to be subject to freezes for an indefinite time period. .

Luxembourg's laws facilitating international cooperation in money laundering include the Act of August 8, 2000, which enhances and simplifies procedures on international judicial cooperation in criminal matters; and the Law of June 14, 2001, which ratifies the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. During its EU Presidency, Luxembourg shepherded the draft of the Third Money Laundering and Terrorist Financing Directive through the EU's legislative process. Luxembourg expects to transpose this Directive into national law in 2008 with the passage of Bill 5811.

Luxembourg cooperates with, and provides assistance to foreign governments in their efforts to trace, freeze, seize and forfeit assets. During 2007, Luxembourg responded to four mutual legal assistance treaty requests from the U.S. and in return requested U.S. government assistance in three cases. Dialogue and other bilateral proceedings between Luxembourg and the United States have been extensive. Upon request from the United States, Luxembourg froze the bank accounts of individuals suspected of involvement in terrorism. Luxembourg also worked closely with the U.S. Department of Justice throughout 2007, on several drug-related money laundering cases as well as one possible terrorist financing case. In October 2006, the United States and Luxembourg announced a sharing agreement in which they would divide equally 11,366,265 euros (then approximately $14,548,820) of forfeited assets of two convicted American narcotics traffickers who had deposited the monies in Luxembourg bank accounts. Luxembourg has placed a priority on progressing with the legal instruments implementing the extradition and mutual legal assistance agreements the United States signed with the European Union in 2003. In December 2007, the Luxembourg Parliament gave final approval to both the bilateral U.S.-Luxembourg and multilateral U.S.-EU extradition and mutual legal assistance agreements.

Luxembourg is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism but has not yet ratified the UN Convention against Transnational Organized Crime. On November 6, 2007, Luxembourg ratified the UN Convention against Corruption.

Luxembourg is a member of the Financial Action Task Force (FATF), which, in a 2004 report, commented that Luxembourg was "broadly compliant with almost all of the FATF Recommendations." The Luxembourg FIU is a member of the Egmont Group. Luxembourg and the United States have had a mutual legal assistance treaty (MLAT) since February 2001. Luxembourg has consistently provided training and assistance in money laundering matters to officials in countries whose regimes are in the development stage.

The Government of Luxembourg has enacted laws and adopted practices that help prevent the abuse of its bank secrecy laws and has enacted a comprehensive legal and supervisory anti-money laundering regime. Luxembourg has steadily enacted AML/CTF laws, policies, and procedures. However, the scarce number of financial crime cases is of concern, particularly for a country that has such a large financial sector. Luxembourg should take action to delineate in legislation regulatory, financial intelligence, and prosecutorial activities among governmental entities in the fight against money laundering and terrorist financing. The situation is most acute regarding the lack of a distinct legal framework for the FIU whose staff, activities, and authorities are divided among at least four different ministries. The State Prosecutors in the FIU should be exempt from nonfinancial crime duties and the FIU should increase the number of analytical staff to effectively analyze and disseminate the volume of STRs that the FIU receives. Luxembourg should pass legislation creating the authority for it to independently designate those who finance terrorism. Luxembourg would be well served to have the authority to designate suspected terrorists. Luxembourg should also enact legislation to address the continued use of bearer shares and consider specifically extending AML legislation to include SICAR entities. Luxembourg should become a party to the UN Convention against Transnational Organized Crime.

## Macau

Under the one country/two systems principle that underlies Macau's 1999 reversion to the People's Republic of China, Macau has substantial autonomy in all areas of governance except defense and foreign affairs. Macau's free port, a lack of foreign exchange controls, limited institutional capacity and a rapidly expanding economy based on gambling and tourism create an environment that can be exploited for money laundering purposes. Macau is a gateway to China, and can be used as a transit point to remit funds and criminal proceeds to and from China. Macau's economy is heavily dependent on gaming. The gaming sector continues to be a significant vulnerability. Macau's offshore financial sector is not fully developed.

The primary money laundering methods in Macau's financial system are wire transfers; currency exchange/cash conversion; bulk movement of cash; the use of casinos to remit or launder money; and the use of nominees, trusts, family members, or third parties to transfer cash. Most of these cases are related to financial fraud, bribery, embezzlement, organized crime, counterfeiting, and drug-related crimes. There have been no reported instances of terrorism-related financial crimes. Crimes related to financial fraud appear to be increasing, while drug-related crimes are becoming less common.

Macau has taken several steps over the past three years to improve its institutional capacity to tackle money laundering. On March 23, 2006, the Macau Special Administrative Region (MSAR) Government passed a 12-article bill on the prevention and repression of money laundering that incorporates aspects of the revised FATF Forty Recommendations. The law expands the number of sectors covered by Macau's previous anti-money laundering (AML) legislation, includes provisions on due diligence, and broadens the definition of money laundering to include all serious predicate crimes.

The AML law also authorizes the establishment of a financial intelligence unit (FIU), which began operations in November 2006. The law provides for 2-8 years imprisonment for money laundering offenses, and if a criminal is involved in organized crime or triad-related money laundering, increases the penalties by one-half. The new law also allows for fines to be added to the time served and eliminates a provision reducing time served for good behavior.

The 2006 law also extends the obligation of suspicious transaction reporting to lawyers, notaries, accountants, auditors, tax consultants and offshore companies. Covered businesses and individuals must meet various obligations, such as the duty to confirm the identity of their clients and the nature of their transactions. Businesses must reject clients that refuse to reveal their identities or type of business dealings. The law obliges covered entities, including casinos, to send suspicious transaction reports (STRs) to the relevant authorities and cooperate in any follow-up investigations.

On March 30, 2006, the MSAR also passed new counterterrorism legislation aimed at strengthening measures to counter terrorist financing (CTF). The law partially implements UNSCR 1373 by making it illegal to conceal or handle finances on behalf of terrorist organizations. Individuals are liable even if they are not members of designated terrorist organizations themselves. The legislation also allows prosecution of persons who commit terrorist acts outside of Macau in certain cases, and would mandate stiff penalties. However, the legislation does not authorize the freezing of terrorist assets outside normal legal channels, nor does it discuss international cooperation on terrorist financing. In January 2005, the Monetary Authority of Macau issued a circular to all banks and other authorized institutions requiring them to maintain a database of suspected terrorists and terrorist organizations.

Macau's financial system is governed by the 1993 Financial System Act and amendments, which lay out regulations to prevent use of the banking system for money laundering. The Act imposes requirements for the mandatory identification and registration of financial institution shareholders, customer identification, and external audits that include reviews of compliance with anti-money laundering statutes. The 1997 Law on Organized Crime criminalizes money laundering for the proceeds of all domestic and foreign criminal activities, and contains provisions for the freezing of suspect assets and instrumentalities of crime. Legal entities may be civilly liable for money laundering offenses, and their employees may be criminally liable.

The 1998 Ordinance on Money Laundering sets forth requirements for reporting suspicious transactions to the Judiciary Police and other appropriate supervisory authorities. These reporting requirements apply to all legal entities supervised by the regulatory agencies of the MSAR, including pawnbrokers, antique dealers, art dealers, jewelers, and real estate agents. In October 2002, the Judiciary Police set up the Fraud Investigation Section to receive suspicious transaction reports (STRs) in Macau and to undertake subsequent investigations. In 2006, the newly established Financial Intelligence Unit (FIU) assumed responsibility for receiving STRs and forwarding actionable reports to the Judiciary Police for investigation. In November 2003, the Monetary Authority of Macau issued a circular to banks, requiring that STRs be accompanied by a table specifying the transaction types and money laundering methods, in line with the collection categories identified by the Asia/Pacific Group on Money Laundering. Macau law provides for forfeiture of cash and assets that assist in or are intended for the commission of a crime. There is no significant difference between the regulation and supervision of onshore and of offshore financial activities.

On September 15, 2005, the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN) designated Macau-based Banco Delta Asia (BDA) as a primary money laundering concern under Section 311 of the USA PATRIOT Act and issued a proposed rule regarding the bank, In its designation of BDA as a primary money laundering concern, FinCEN cited in the Federal Register that "the involvement of North Korean Government agencies and front companies in a wide variety of illegal activities, including drug trafficking and the counterfeiting of goods and currency" and noted that North Korea has been positively linked to nearly 50 drug seizures in 20 different countries since

1990. Following an investigation of BDA conducted with the cooperation of the Macanese authorities, Treasury finalized the Section 311 rule in March 2007, prohibiting U.S. financial institutions from opening or maintaining correspondent accounts for or on behalf of BDA. This rule remains in effect.

Shortly after the U.S. designation, The Monetary Authority took control of Banco Delta Asia and froze approximately U.S. $25 million in accounts linked to North Korea. The Government of Macau announced in March 2007 that it would continue to maintain control over Banco Delta Asia for at least six more months to resolve the Banco Delta Asia situation. In April, 2007, the Macanese authorities released the $25 million North Korean-related funds frozen at BDA. In September, 2007, The Treasury Department's Financial Crimes Enforcement Network denied two petitions filed on behalf of BDA and its owners to lift the Section 311 Final Rule designating BDA as a "primary money laundering concern." On September 30, 2007 Macau Monetary Authority announced that Banco Delta Asia would be returned immediately to its shareholders, but continued international restrictions on BDA and its subsidiaries outside of Macau that limit BDA to pataca currency business in Macau.

A Macau Monetary Authority official serves as the head of the FIU. As of October 2007, in addition to the FIU Head, the staff consisted of two officials (seconded from the Insurance Bureau and the Monetary Authority), a judiciary police official, and two information technology staff. The FIU works with the Macau Judicial Police on investigation of suspicious transaction reports (STRs) and with the Public Prosecutors Office on prosecution of offenders. The FIU moved into permanent office space in January 2007 and is accepting STRs from banks, financial institutions and the Gaming Inspectorate.

The gaming sector and related tourism are critical parts of Macau's economy. Taxes from gaming in the first eleven months of 2007 increased by 48.3 percent from the same period in 2006 and comprised 71percent of government revenue in the first eleven months of 2007. Gaming revenue in the first nine months of 2007 exceeded the 2006 total and account for well over 50 percent of Macau's GDP. The MSAR ended a long-standing gaming monopoly early in 2002 when it awarded concessions to two additional operators, the U.S.-based Las Vegas Sands and Wynn Corporations. Macau now effectively has six separate casino licensees operating 28 casinos: three concession holders Sociedade de Jogos de Macau (SJM), Galaxy and Wynn: and three sub concession holders: Las Vegas Sands, MGM and PBL/Melco. Las Vegas Sands opened its first casino, the Sands, on May 18, 2004 and its second the Venetian-Macao in September 2007. MGM opened its first Macau casino in December 2007. Wynn opened its casino in September 2006. A consortium including Australia's PBL and Macau's Melco operates the Crown casino, which opened in May 2007 and runs several slot machine rooms in Macau. Rapid expansion of the gaming industry in Macau continues; several additional casinos are expected to open in the next few years.

Under the old monopoly framework, organized crime groups were closely associated with the gaming industry through their control of VIP gaming rooms and activities such as racketeering, loan sharking, and prostitution. The VIP rooms catered to clients seeking anonymity within Macau's gambling establishments, and received minimal official scrutiny. As a result, the gaming industry provided an avenue for the laundering of illicit funds and served as a conduit for the unmonitored transfer of funds out of China. VIP rooms continue to operate and are the primary revenue generators for Macau's casinos. Although the arrival of international gaming companies has improved management and governance in all aspects of casino operations, concerns about organized crime groups and poorly regulated junket operators associations with VIP rooms remain. The MSAR's money laundering legislation aims to make money laundering by casinos more difficult by improving oversight, and tightening reporting requirements. On June 7, 2004, Macau's Legislative Assembly passed legislation allowing casinos and junket operators to make loans, in chips, to customers, in an effort to prevent loan-sharking. The law requires both casinos and junket operators to register with the government.

The Macau criminal code (Decree Law 58/95/M of November 14, 1995, Articles 22, 26, 27, and 286) criminalizes terrorist financing. Macau does not have any provision or procedures for freezing terrorist

related funds or assets to fully implement UNSCRs 1267 and 1373. However, although no special mechanism exists and a judicial order is required, the general framework of seizure and forfeiture of funds and assets under the Criminal Code and Criminal Procedure Code do provide the MSAR the authority to freeze terrorist assets. Macau financial authorities direct the institutions they supervise to conduct searches for terrorist assets, using the consolidated list provided by the UN 1267 Sanctions Committee and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. No terrorist assets were identified in 2007.

The Macau legislature passed a counter-terrorism law in April 2002 to facilitate Macau's compliance with UNSCR 1373. The legislation criminalizes violations of UN Security Council resolutions, including counterterrorism resolutions, and strengthens counter-terrorist financing provisions. When China ratified the UN International Convention for the Suppression of the Financing of Terrorism, China stipulated that the Convention would apply to the MSAR

Increased attention to financial crimes in Macau since the events of September 11, 2001, has led to a general increase in the number of suspicious transaction reports (STRs); however, the number of STRs remains relatively low. Macau's Judiciary Police received 109 STRs in 2004, 194 in 2005, 396 STRs from January to September 2006, and 557 STRs from January to September 2007. In 2004 Macau opened ten money laundering cases but prosecuted none. In 2005 Macau opened nine money laundering cases and prosecuted two. Since the entry into force of the new AML law in April 2006, the Macau Public Prosecutions office has received 23 suspected cases of money laundering from the FIU. Of these, 14 have been referred for investigation by the Judicial Police or the Commission Against Corruption. Since 2005, the Judicial Police have referred three money laundering cases to the Public Prosecutions office.

In May 2002, the Macau Monetary Authority revised its anti-money laundering regulations for banks to bring them into greater conformity with international practices. Guidance also was issued for banks, moneychangers, and remittance agents, addressing record keeping and suspicious transaction reporting for cash transactions over U.S. $2,500. For such transactions, banks, insurance companies, and moneychangers must perform customer due diligence. However for casinos, Macau requires customer due diligence only for transactions above U.S. $62,500. In 2003, the Macau Monetary Authority examined all moneychangers and remittance companies to determine their compliance with these regulations. The Monetary Authority of Macau, in coordination with the IMF, updated its bank inspection manuals to strengthen anti-money laundering provisions. The Monetary Authority inspects banks every two years, including their adherence to anti-money laundering regulations. There is no requirement to report large sums of cash carried into Macau. The Macau Customs Service has the authority to conduct physical searches and detain suspicious persons and executes random checks on cross-border movement of cash, including record keeping when the amount of cash carried over the border exceeds US$38,500. However, there is no central database for such reports. Mainland China does restrict the transport of RMB out of China. Persons may carry no more than RMB 20,000 (approximately U.S. $2,750) per day out of China. According to the Macau Prosecutors Office, this Chinese requirement limits the number of people carrying large amounts of cash into Macau.

The United States has no law enforcement cooperation agreements with Macau, though informal cooperation between the United States and Macau routinely takes place. The Judiciary Police have been cooperating with law enforcement authorities in other jurisdictions through the Macau branch of Interpol, to suppress cross-border money laundering. In addition to Interpol, the Fraud Investigation Section of the Judiciary Police has established direct communication and information sharing with authorities in Hong Kong and Mainland China. In July 2006, the MSAR enacted the Law on Judicial Cooperation in Criminal Matters, enabling the MSAR to enter into more formal judicial and law enforcement cooperation relationships with other countries. The law became effective in November 2006. Macau's FIU has not yet established MOUs on information sharing with other jurisdictions but is currently negotiating with FIUs from Hong Kong, China, Portugal, Japan, Korea, and Sri Lanka.

The Monetary Authority of Macau also cooperates internationally with other financial authorities. It has signed memoranda of understanding with the People's Bank of China, China's Central Bank, the China Insurance Regulatory Commission, the China Banking Regulatory Commission, the Hong Kong Monetary Authority, the Hong Kong Securities and Futures Commission, the Insurance Authority of Hong Kong, and Portuguese bodies including the Bank of Portugal, the Banco de Cabo Verde and the Instituto de Seguros de Portugal.

Macau participates in a number of regional and international organizations. It is a member of the Asia/Pacific Group on Money Laundering (APG), the Offshore Group of Banking Supervisors, the International Association of Insurance Supervisors, the Offshore Group of Insurance Supervisors, the Asian Association of Insurance Commissioners, the International Association of Insurance Fraud Agencies, and the South East Asia, New Zealand and Australia Forum of Banking Supervisors (SEAZA). In 2003, Macau hosted the annual meeting of the APG, which adopted the revised FATF Forty Recommendations and a strategic plan for anti-money laundering efforts in the region from 2003 to 2006. In ratifying the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption China in each case specified that the treaty would apply to the MSAR. Macau officials have taken a number of steps in the past three years to raise industry awareness of money laundering. The Macau Monetary Authority trains banks on anti-money laundering measures on a regular basis.

In December 2006, the Asia Pacific Group (APG) and Offshore Group of Banking Supervisors (OGBS) conducted a joint Mutual Evaluation of the anti-money laundering and combating the financing of terrorism measures in place in Macau The Mutual Evaluation Report stated that Macau was noncompliant with FATF Special Recommendation IX, in that Macau should have measures in place to detect the physical cross border transport of currency and bearer-negotiable instruments. Macau does not require reporting of the movement of currency above any threshold level across its borders, or reporting of large currency transactions above any threshold level. Macau's AML/CTF regime is also deficient in a number of other respects, including: the lack of a mechanism to confiscate, freeze, and forfeit proceeds of crime independent of criminal process; the lack of ability to freeze terrorist funds; failure to establish an independent FIU, which was established only as a special project entity with a term of three years; the lack of requirements for financial institutions to verify the identify of persons on whose behalf a customer is acting to understand the ownership and control structure of customers, or to examine the background and purpose of transactions with no economic or visible lawful purpose; the failure to develop a risk assessment of, and risk based approach to the gaming sector; and the lack of adequate legal framework for requiring Designated Non-Financial Business and Professions, including casinos and gaming concessionaires to report suspicious transactions.

Macau should continue to improve its ability to implement and enforce existing laws and regulations. Macau should ensure that regulations, structures, and training are adequate to prevent money laundering in the gaming industry, including implementing regulations to prevent money laundering in casinos, especially regulations to improve oversight of VIP rooms. The MSAR should take steps to implement the new FATF Special Recommendation IX, adopted by the FATF in October 2004, requiring countries to put in place detection and declaration systems for cross-border bulk currency movement. Macau should establish asset freezing mechanisms and procedures to fully implement UN Security Council Resolutions 1267 and 1373. This process should not be linked to the criminal process and should include the ability to freeze terrorist assets without delay. Macau should increase public awareness of the money laundering problem, improve interagency coordination and training, and boost cooperation between the MSAR and the private sector in combating money laundering. Macau should institutionalize its Financial Intelligence Unit by making it a permanent, statutory body and ensure the FIU meets Egmont Group standards for information sharing. Macau's Judicial Police have limited

resources devoted to AML/CTF investigations. Additional manpower would allow for more investigations and enforcement action.

## Malaysia

Malaysia is not a regional center for money laundering. A range of significant money laundering and terrorist financing risks in Malaysia are being addressed through the implementation of the country's Anti-Money Laundering Act and other AML/CTF measures. Malaysia has long porous land and sea borders and its open economy and strategic geographic position influence money laundering and terrorist finance in the region. Drug trafficking is the main source of illegal proceeds in Malaysia. Malaysia is primarily used as a transit country to transfer drugs originating from the Golden Triangle and Europe, including heroin, amphetamine type substances and ketamine. Authorities also highlight illegal proceeds from corruption as well as a wide range of predicate offenses including fraud, illegal gambling, credit card fraud, counterfeiting, forgery, human trafficking, extortion, and smuggling. Money laundering techniques include placing criminal proceeds into the banking system, using nominees, the use of front companies, purchasing insurance products and high value goods and real property, investment in capital markets, and the use of moneychangers. Smuggling of goods subject to high tariffs is a major source of illicit funds. Malaysia has a significant informal remittance sector.

The GOM has a well-developed AML/CTF framework. Malaysia's National Coordination Committee to Counter Money Laundering (NCC), comprised of members from 13 government agencies, oversaw the drafting of Malaysia's Anti-Money Laundering Act of 2001 (AMLA). The NCC is responsible for the development of the national AML/CTF program, including the coordination of national-wide AML/CTF efforts.

In February 2007, the APG conducted its second Mutual Evaluation on Malaysia. The evaluation was based on all FATF recommendations; Malaysia received ratings of "compliant" or "largely compliant" on 33 of the 49 FATF Recommendations, 15 ratings of "partially compliant;" and one rating of "noncompliant" with Special Recommendation on Terrorist Financing IX on cash couriers.

Subsequent to the mutual evaluation, the NCC established a task force comprised of the Royal Malaysian Customs, Immigration Department, Ministry of Internal Security, and Bank Negara Malaysia to formulate action plans to achieve full compliance with Special Recommendation IX. Malaysia's relatively lax customs inspection at ports of entry and its extensive coastlines, particularly along the east coast of Sabah in Borneo, serve to increase its vulnerability to smuggling, including cash smuggling.

On March 6, 2007, Malaysia enacted amendments to five different pieces of legislation: the AMLA, now called the Anti-Money Laundering and Anti-Terrorism Financing Act (AMLATF), the Penal Code, the Subordinate Courts Act, the Courts of Judicature Act, and the Criminal Procedure Code. These amendments impose penalties for terrorist acts, allow for the forfeiture of terrorist-related assets, allow for the prosecution of individuals who have provided material support for terrorists, expand the use of wiretaps and other surveillance of terrorist suspects, and permit video testimony in terrorist cases.

In 2002, the AMLA provided for the establishment of a financial intelligence unit in Malaysia. The Unit Perisikan Kewangan (UPW), located in the Central Bank, Bank Negara Malaysia (BNM), is tasked with receiving and analyzing information, and sharing financial intelligence with the appropriate enforcement agencies for further investigations. The UPW cooperates with other relevant agencies to identify and investigate suspicious transactions. A comprehensive supervisory framework has been implemented to audit financial institutions' compliance with the AMLA and its subsidiary legislation and relevant guidelines. Currently, BNM maintains 383 examiners who are responsible for money laundering inspections for both onshore and offshore financial institutions.

Malaysia's financial institutions have strict "know your customer" rules under the AMLA. Every transaction, regardless of its size, is recorded. Reporting institutions must maintain records for at least six years and report any suspicious transactions to the UPW. If the reporting institution deems a transaction suspicious it must report that transaction to the UPW promptly regardless of the transaction size. In addition, cash threshold reporting (CTR) requirements above RM 50,000 (approximately U.S. $14,900) were imposed upon banking institutions effective as of September 2006. UPW officials indicate that they receive regular reports from the AMLA reporting institutions. Reporting individuals and their institutions are protected by statute with respect to their cooperation with law enforcement. While Malaysia's bank secrecy laws prevent general access to financial information, those secrecy provisions are overridden in the case of reporting of suspicious transactions or criminal investigations.

Malaysia has adopted banker negligence (due diligence) laws that make individual bankers responsible if their institutions launder money or finance terrorists. Both reporting institutions and individuals are required to adopt internal compliance programs to guard against any offense. Under the AMLA, any person or group that engages in, attempts to engage in, or abets the commission of money laundering or financing of terrorism is subject to criminal sanction. All reporting institutions are subject to review by the UPW. Under the AMLA, reporting institutions include financial institutions from the conventional, Islamic, and offshore sectors as well as nonfinancial businesses and professions such as lawyers, notaries public, accountants, company secretaries, and Malaysia's one licensed casino. In 2005, reporting obligations were imposed upon licensed gaming outlets, notaries public, offshore trading agents, and listing sponsors. Phased-in reporting requirements for stock brokers and futures brokers were expanded in 2005, and in 2006, reporting requirements were extended to money lenders, pawnbrokers, registered estate agents, trust companies, unit trust management companies, fund managers, futures fund managers, nonbank remittance service providers, and nonbank affiliated issuers of debit and credit cards. In 2007, the AMLA was further extended to insurance financial advisers, moneylenders in the state of Sabah, E-money issuers and leasing and factoring businesses.

In mid-2007, Islamic banking assets were RM 144 billion (approximately U.S. $43 billion), accounting for 12 percent of the total assets in the banking sector, up from 11.8 percent in mid-2006 and 11.6 percent in mid-2005. Malaysia's growing Islamic finance sector is subject to the same supervision to combat financial crime as the commercial banks.

In 1998, Malaysia imposed foreign exchange controls that restricted the flow of the local currency from Malaysia. Onshore banks must record cross-border transfers over RM 10,000 (approximately U.S. $3,000). An individual form is completed for each transfer above RM 200,000 (approximately U.S. $60,000). The thresholds for the bulk register for transactions were raised in October 2007. Recording is now done in a bulk register for transactions between U.S. $3,000 and $60,000. Banks are obligated to record the amount and purpose of these transactions.

While Malaysia's offshore banking center on the island of Labuan has different regulations for the establishment and operation of offshore businesses, it is subject to the same anti-money laundering laws as those governing onshore financial service providers. Malaysia's Labuan Offshore Financial Services Authority (LOFSA) serves as a member of the Offshore Group of Banking Supervisors. Offshore banks, insurance companies, trust companies, trading agents, and listing sponsors are required to file suspicious transaction reports under the country's anti-money laundering law. LOFSA is under the authority of the Ministry of Finance and works closely with BNM. LOFSA licenses offshore banks, banking companies, trusts, and insurance companies and performs stringent background checks before granting an offshore license. The financial institutions operating in Labuan are generally among the largest international banks and insurers. Nominee (anonymous) directors are not permitted for offshore banks, trusts or insurance companies. Labuan had 6,152 registered offshore companies as of September 30, 2007. Bearer instruments are strictly prohibited in Labuan.

Offshore companies must be established through a trust company. Trust companies are required by law to establish true beneficial owners and submit suspicious transaction reports. There is no requirement to publish the true identity of the beneficial owner of international corporations; however, LOFSA requires all organizations operating in Labuan to disclose information on its beneficial owner or owners, as part of its procedures for applying for a license to operate as an offshore company. LOFSA maintains financial information on licensed entities, releasing it either with the consent of those entities or upon investigation.

In November 2005, LOFSA revoked the license of the "Blue Chip Pathfinder" Private Fund for "evidence that Swift Securities Investments Ltd had contravened the terms of the consent and acted in a manner that was detrimental to the interests of mutual fund investors." The Fund has since been terminated. Also in 2005, LOFSA revoked the investment banking license of Swift Securities Investments Ltd for "contravening the provisions of the license."

In April 2006, LOFSA announced that it had subscribed to a service which provides structured intelligence on high and heightened risk individuals and entities, including terrorists, money launderers, politically exposed persons, arms dealers, sanctioned entities, and others, to gather information on their networks and associates. LOFSA now uses this service as part of its licensing application process.

The Free Zone Act of 1990 is the enabling legislation for free trade zones in Malaysia. The zones are divided into Free Industrial Zones (FIZ), where manufacturing and assembly takes place, and Free Commercial Zones (FCZ), generally for warehousing commercial stock. The Minister of Finance may designate any suitable area as an FIZ or FCZ. Currently there are 13 FIZs and 12 FCZs in Malaysia. The Minister of Finance may appoint any federal, state, or local government agency or entity as an authority to administer, maintain, and operate any free trade zone. Companies wishing to operate in an FTZ or FCZ must apply for a license and be approved. The time needed to obtain such licenses from the administrative authority to operate in a particular free trade zone depends on the type of activity. Clearance time ranges from two to eight weeks. There is no indication that Malaysia's free industrial and free commercial zones are being used for trade-based money laundering schemes or by the financiers of terrorism. Rather, these zones are dominated by large international manufacturers such as Dell and Intel, which are attracted to the zones because they offer preferential tax and tariff treatment.

The UPW has been a member of the Egmont Group since July 2003. Prior to 2007, UPW had signed memoranda of understanding (MOUs) on the sharing of financial intelligence with the FIUs of Australia, Indonesia, Thailand, the Philippines and China. In 2007,and early 2008, an additional seven MOUs were signed with the United Kingdom, United States, Japan, Republic of Korea, Sweden, Chile and Sri Lanka. Malaysia is a member of the Asia/Pacific Group (APG) on Money Laundering, a FATF-style regional body.

In April 2002, the GOM passed the Mutual Assistance in Criminal Matters Act (MACMA), and in July 2006 concluded a Mutual Legal Assistance Treaty with the United States. Malaysia concluded a similar treaty among like-minded ASEAN member countries in November 2004. In October 2006, Malaysia ratified treaties with China and Australia regarding the provision of mutual assistance in criminal matters. An extradition treaty was also signed with Australia. The mutual assistance treaties enable States Parties to assist each other in investigations, prosecutions, and proceedings related to criminal matters, including terrorism, drug trafficking, fraud, money laundering and human trafficking.

Malaysia made its first money laundering arrest in 2004. As of October 2007, the Attorney General's Chambers had prosecuted 29 money laundering cases, involving a total of 829 charges with a cumulative total of RM 273.6 million (approximately U.S. $83.7 million). Out of the 29 cases, there were three convictions.

Malaysia is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. Malaysia has signed but has not yet ratified the UN Convention against Corruption. On May 29, 2007, the Government of Malaysia (GOM) became a party to the UN International Convention for the Suppression of the Financing of Terrorism.

The GOM has cooperated closely with U.S. law enforcement in investigating terrorist-related cases since the signing of a joint declaration to combat international terrorism with the United States in May 2002. The GOM recently improved legislation enabling it to comprehensively freeze assets under the UNSCRs 1267 and 1373. The Ministry of International Security has the authority to identify and freeze the assets of terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and, whenever a new designee is added, the UPW issues immediate orders to all licensed financial institutions, both onshore and offshore, to do so. At the same time, the UPW also disseminates information on persons and entities designated unilaterally by other countries, including the United States, to these institutions. Since 2003 Bank Negara Malaysia has issued 43 circulars and nine accounts have been frozen amounting to approximately U.S. $76,400.

Malaysian authorities have highlighted risks from terrorist groups and terrorist financing. A number of terrorist organizations have been active on Malaysian territory, and authorities have taken action against Jemaah Islamiah. Terrorist financing in Malaysia is predominantly carried out using cash and relies on trusted networks. While Malaysia has recently improved the legislative framework to criminalize terrorist financing, there have been no investigations, prosecutions or convictions relating to terrorist financing under this new scheme. The Ministry of Foreign Affairs opened the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT) in August 2003. SEARCCT coordinates courses and seminars on combating terrorism and terrorist finance.

The GOM has rules regulating charities and other nonprofit entities. The Registrar of Societies is the principal government official who supervises and controls charitable organizations, with input from the Inland Revenue Board (IRB) and occasionally the Companies Commission of Malaysia (CCM). The Registrar mandates that every registered society of a charitable nature submit its annual returns, including its financial statements. Should activities deemed suspicious be found, the Registrar may revoke the nonprofit organization's (NPO) registration or file a suspicious transaction report. Registering as a NPO can be bureaucratic and time-consuming. One organization reported that getting registered took nine months and required multiple personal interviews to answer questions about its mission and its methods. Some NPOs reportedly register as "companies" instead, a quick and inexpensive process requiring capital of approximately 60 cents and annual financial statements.

In March 2006, the UPW completed a review of the nonprofit sector with the Registrar, the IRB, and the CCM, in an effort to ensure that the laws and regulations were adequate to mitigate the risks of nonprofit organizations as conduits for terrorist financing. BNM reports that the review did not show any significant regulatory weaknesses; however, the GOM is considering measures to enhance the monitoring of fundraising, including increased disclosure requirements of how funds are spent.

Malaysia's tax law allows a tax credit, which encourages the reporting of contributions, for Zakat (alms) to mosques or registered Islamic charitable organizations. Islamic Zakat contributions can be taken as payroll deductions, which help prevent the abuse of charitable giving. There is no similar tax credit for nonMuslims.

The Government of Malaysia should continue to enhance its cooperation on a regional, multilateral, and international basis. The GOM should improve enforcement of regulations regarding its free trade zones, which remain vulnerable to the financing of terrorism and money laundering. Given that cash smuggling is a major method used by terrorist financers to move money in support of their activities, as a priority matter, Malaysian authorities should establish and adhere to a cross border currency declaration system that meets purpose and intent of the FATF Special Recommendation IX on bulk cash smuggling. There is a significant informal remittance sector in Malaysia that is not subject to

AML/CTF controls and which may be vulnerable to misuse for money laundering and terrorist financing. Law enforcement and customs authorities should examine trade based money laundering and invoice manipulation and their relationship to underground finance and informal remittance systems. Malaysia should ratify the UN Convention against Corruption.

## Mexico

Mexico is a major drug-producing and drug-transit country. It also serves as one of the major conduits for proceeds from illegal drug sales leaving the United States. The illicit drug trade is the principal source of funds laundered through the Mexican financial system. Other major sources of illegal proceeds being laundered include corruption, kidnapping, trafficking in firearms and immigrants, and other crimes. The smuggling of bulk shipments of U.S. currency into Mexico and the movement of the cash back into the United States via couriers, armored vehicles, and wire transfers remain favored methods for laundering drug proceeds.

According to U.S. law enforcement officials, Mexico remains one of the most challenging money laundering jurisdictions for the United States, especially with regard to the investigation of money laundering activities involving the cross-border smuggling of bulk currency derived from drug transactions and other transnational criminal activity. Sophisticated and well-organized drug trafficking organizations based in Mexico are able to take advantage of the extensive U.S.-Mexico border and the large flow of licit remittances. In addition, the combination of a sophisticated financial sector and relatively weak regulatory controls facilitates the concealment and movement of drug proceeds. U.S. officials estimate that since 2003, as much as U.S. $22 billion may have been repatriated to Mexico from the United States by drug trafficking organizations. In April 2006, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) issued a warning to the U.S. financial sector on the potential use of certain Mexican financial institutions, including Mexican casas de cambio (licensed foreign exchange offices) and centros cambiarios (unlicensed foreign exchange offices), to facilitate bulk cash smuggling. Corruption is also a concern: in recent years, various Mexican officials have come under investigation for alleged money laundering activities.

Currently, there are 39 commercial banks and 71 foreign financial representative offices operating in Mexico, as well as 94 insurance companies, 160 credit unions, and 25 casas de cambio. Commercial banks, foreign exchange companies, and general commercial establishments are allowed to offer money exchange services. Although the underground economy is estimated to account for 20-40 percent of Mexico's gross domestic product, the informal economy is considered to be much less significant with regard to money laundering than the criminal-driven segments of the economy. Beginning in 2005, permits were issued for casinos to operate in Mexico. National lotteries, horse races, and sport pools are also legal. Casinos, as well as offshore banks, lawyers, accountants, couriers, and brokers, are currently not subject to anti-money laundering reporting requirements.

From 2000 to 2006, remittances from the United State to Mexico grew from U.S. $6.6 billion to nearly U.S. $24 billion a year; in 2007, the increase is estimated at less than two percent. Many U.S. banks have partnered with their Mexican counterparts to develop systems to simplify and expedite the transfer of money, including wider acceptance by U.S. banks of the "matricula consular," an identification card issued by Mexican consular offices to Mexican citizens residing in the United States that has been criticized as insecure. In some cases, the sender or the recipient can simply provide the matricula consular as identification to execute a remittance, often without having to open a bank account. While this makes licit remittances more accessible, it also leaves the system open to potential money laundering and exploitation by organized crime groups. The U.S. Embassy estimates that in 2007, electronic transfers accounted for 90 percent of all remittances to Mexico. It is likely that few first-tier commercial banks will reach down to serve low-income clients who receive such remittances, with cajas populares and cajas solidarias (financial cooperatives that function as credit

unions) being the likely candidates to fill this gap. This presents a new set of concerns over whether this system will present potential money laundering opportunities for bulk currency transactions.

The Tax Code and Article 400 bis of the Federal Penal Code criminalize money laundering related to any serious crime. Money laundering is punishable by imprisonment of five to fifteen years and a fine. Penalties are increased when a government official in charge of the prevention, investigation, or prosecution of money laundering commits the offense. Mexico's all-crimes approach to money laundering criminalizes the laundering of the proceeds of any intentional act or omission, regardless of whether or not that act or omission carries a prison term. Rather than applying to proceeds of criminal offenses, the statute applies to "the proceeds of an illicit activity", which is defined as resources, rights, or goods of any nature for which there exists well-founded certainty that they are derived directly or indirectly from or represent the earnings derived from the commission of any crime, and for which no legitimate origin can be established. This construction of the predicate offense allows prosecutors, upon demonstrating criminality, to shift the burden of proof to the defendant to establish the legitimate origin of the property. An offense committed outside of Mexico may also constitute a predicate for money laundering offense. Because criminal proceeds generated abroad would have an effect in Mexico when laundered in or through its national territory, the laundering of those proceeds could be prosecuted under Mexican law.

The Banking and Securities Commission (CNBV) regulates and supervises banks, limited scope financial companies, securities brokerage firms, foreign exchange firms, and mutual funds. The Tax Authority (SAT) supervises nonlicensed foreign exchange retail centers and money remitters. The CNBV has the remit to impose administrative sanctions for noncompliance, revoke licenses, and conduct on-site inspections and off-site monitoring of regulated entities. The CNBV is also responsible for issuing regulations. Regulations require banks and other financial institutions (including mutual savings companies, insurance companies, securities brokers, retirement and investment funds, financial leasing and factoring funds, casas de cambio, centros cambiarios, and money remittance businesses) to know and identify customers and maintain records of transactions.

In 2004, the Ministry of the Treasury (SHCP) reorganized and renamed its financial intelligence unit (FIU), the Unidad de Inteligencia Financiera (UIF). The UIF's personnel number approximately 50 and are comprised mostly of forensic accountants, lawyers, and analysts. Regulated entities must report to the UIF any suspicious transactions, currency transactions over U.S. $10,000 (except for centros cambiarios, which are subject to a U.S. $3,000 threshold), and transactions involving employees of financial institutions who engage in suspicious activity. Banks also require occasional customers performing transactions equivalent to or exceeding U.S. $3,000 in value to be identified, so that the transactions can be aggregated daily to prevent circumvention of the requirements to file cash transaction reports (CTRs) and suspicious transaction reports (STRs). A 2005 provision of the tax law requires real estate brokerages, attorney, notaries, accountants, and dealers in precious metals and stones to report all transactions exceeding U.S. $10,000 to the SAT, which shares that information with the UIF. In 2006, nonprofit organizations were made subject to reporting requirements for donations greater than U.S. $10,000. Financial institutions have also implemented programs for screening new employees and verifying the character and qualifications of their board members and high-ranking officers.

In 2000, Mexico amended its Customs Law to reduce the threshold for reporting inbound cross-border transportation of currency or monetary instruments from $20,000 to $10,000. At the same time, it established a requirement for the reporting of outbound cross-border transportation of currency or monetary instruments of U.S. $10,000 or more. These reports are received by the UIF and cover a wider range of monetary instruments (e.g. bank drafts) than those required by the United States. As a result of the cooperation between Mexican Customs, the Financial Crimes Unit of the Office of the Deputy Attorney General against Organized Crimes (SIEDO), and various U.S. agencies, Mexico has

seized over U.S. $60 million in bulk currency shipments leaving Mexico City's international airport since 2002.

The UIF is responsible for receiving, analyzing, and disseminating STRs and CTRs, as well as reports on the cross-border movements of currency. The UIF also reviews all crimes linked to Mexico's financial system and examines the financial activities of public officials. In 2007, the UIF received approximately 38,400 STRs and 5,607,000 CTRs. Following the analysis of CTRs, STRs, and reports on the cross-border movements of currency, the UIF sends reports that are deemed to merit further investigation, and have been approved by the SHCP's legal counsel, to the Office of the Attorney General (PGR). From 2004 to December 2007, the UIF sent 89 cases to the PGR for its consideration for prosecution. The PGR's special financial crimes unit (within SIEDO) works closely with the UIF in money laundering investigations. UIF personnel also have working-level relationships with other federal law enforcement entities, including the Federal Investigative Agency (AFI) and the Federal Police (PFP), to help it support the PGR's investigations of criminal activities with ties to money laundering. In 2006, the UIF signed Memoranda of Understanding (MOUs) with the Economy Secretariat and the Mexican immigration authorities that provide access to their databases. The UIF has also signed agreements with the CNBV and the National Commission of Insurance and Finance (CNSF) to coordinate to prevent money laundering and terrorist financing. The UIF is currently finalizing similar negotiations with the SHCP and the National Savings Commission (CONSAR).

In 2007, U.S. authorities observed a significant increase in the number of complex money laundering investigations by SIEDO, with support from the UIF and coordinated with U.S. officials. As of November 2007, SIEDO had initiated 142 criminal investigations into money laundering cases, 77 of which were brought to trial. One high profile case was the September 2007 arrest of

Sandra Avila Beltran (also known as the "Queen of the Pacific"), who was indicted in the United States in 2004 on separate drug smuggling charges. Avila Beltran is the niece of drug-kingpin Miguel Angel Felix Gallardo, who is serving a long sentence for drug smuggling and for the 1985 murder of DEA agent Enrique Camarena. She is also the niece of Juan José Quintero Payan, who was extradited to the United States on drug smuggling charges. Avila Beltran shielded her narcotics-related financial activities behind legitimate and successful businesses in Mexico, including a string of tanning and beauty salons and a real estate company with multiple locations. The Government of Mexico (GOM) demonstrated that she had forged cocaine trafficking and financial deals between Mexican and Colombian traffickers over the last decade. The Avila Beltran case highlighted the difficulty of prosecuting those involved in the financial aspects of the drug trade.

Another complex case was the GOM-initiated raids in December against Victor Emilio Cazares Salazar (also known as Victor Emilio Cazares Gastellum), at the same time as the U.S. Treasury's Office of Foreign Assets Control (OFAC) designated his sister, Mexican money launderer Blanca Margarita Cazares Salazar, as a specially designated narcotics traffickers subject to sanctions pursuant to the Foreign Narcotics Kingpin Designation Act. The sequencing represents Mexico's aggressive pursuit of an important money laundering function in conjunction with U.S. Government (USG) efforts, including the February 2007 U.S. indictment of Victor Cazares Salazar. Blanca Cazares Salazar and her widespread money laundering organization acted as fronts for her brother and Mexican drug kingpin Ismael Zambada Garcia (also known as "Mayo Zambada"), leaders of Mexico's Sinaloa Cartel. Victor Emilio Cazares Salazar's narcotics funds spawned a complex, interlocking network of businesses located throughout Mexico, including three Tijuana-based money service businesses and a chain of approximately 20 jewelry and cosmetics boutiques located in eight Mexican states, as well as importation firms, restaurants, mobile phone services, and money service businesses in Sinaloa, Jalisco, Baja California, and Mexico City.

Although the United States and Mexico both have asset forfeiture laws and provisions for seizing assets abroad derived from criminal activity, U.S. requests of Mexico for the seizure, forfeiture, and

repatriation of criminal assets have rarely met with success. Currently, Mexico does not have a civil forfeiture regime and can only forfeit assets upon a final criminal conviction; it can also seize assets administratively if they are deemed to be "abandoned" or unclaimed. Draft legislation pending in the Mexican Congress includes constitutional changes that would enable a forfeiture regime similar to Colombia's law of extinguishment of ownership ("extinción de dominio"). If passed, any asset seizure regime will require considerable implementation efforts.

In 2001, pursuant to a USG request, the GOM seized assets valued at millions of dollars in Mexico from Alyn Richard Wage, who was charged in the United States in a major fraud case (the "Tri-West" case). These assets were found by a U.S. court to be proceeds of the fraud and were the subject of a final order of forfeiture in the United States. For several years, the USG has sought the assistance of the Mexican courts to enforce the U.S. forfeiture order and repatriate the assets to the United States to compensate the victims of the fraud. In October 2007, the PGR filed a petition, with supporting documents from the USG, asking the court to recognize and enforce the U.S. forfeiture order, employing the argument of "abandoned funds." The case remains without resolution.

Another significant case involves Zhenli Ye Gon. Approximately $207 million was seized in March 2007 from his Mexico City residence. The funds seized reportedly included dollars, Mexican pesos, euros, Hong Kong dollars, and Mexican gold bullion coins. GOM authorities also seized two dwellings and seven vehicles. The Drug Enforcement Administration (DEA) has described the seizure as the largest ever of drug money anywhere in the world. These funds have been forfeited under the same argument of "abandoned funds". Zhenli was arrested in the United States in July 2007 and is accused of trafficking tons of pseudoephedrine and other chemicals to supply Mexican methamphetamine labs.

In 2007, after nearly three years of consideration, Mexico criminalized terrorist financing, with punishments of up to 40 years in prison. The new law amends the Federal Penal Code to link terrorist financing to money laundering and establish international terrorism as a predicate crime when it is committed in Mexico to inflict damage on a foreign state. The GOM has responded positively to international and USG efforts to identify and block terrorist-related funds, and it continues to monitor suspicious financial transactions, although no such assets have been frozen to date.

Mexico has developed a broad network of bilateral agreements and regularly meets in bilateral law enforcement working groups with its counterparts within the U.S. law enforcement community. The U.S.-Mexico Mutual Legal Assistance Treaty (MLAT) entered into force in 1991. Mexico and the United States also implement other bilateral treaties and agreements for cooperation in law enforcement issues, including the Financial Information Exchange Agreement (FIEA) and the Memorandum of Understanding (MOU) for the exchange of information on the cross-border movement of currency and monetary instruments.

Mexico is a member of the Financial Action Task Force (FATF) and the Financial Action Task Force for South America (GAFISUD). The GOM currently holds the GAFISUD presidency. In addition to its membership in the FATF and GAFISUD, Mexico participates in the Caribbean Financial Action Task Force (CFATF) as a cooperating and supporting nation. Mexico will undergo a FATF mutual evaluation in January 2008. The UIF is a member of the Egmont Group, and Mexico participates in the Organization of American States' Inter-American Drug Abuse Control Commission's (OAS/CICAD) Experts Group to Control Money Laundering. The GOM is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, the UN International Convention for the Suppression of the Financing of Terrorism, and the Inter-American Convention against Terrorism.

The GOM has made fighting money laundering and drug trafficking one of its top priorities, and has made progress in combating these crimes over the course of 2007. However, Mexico continues to face challenges with respect to is anti-money laundering and counter-terrorist financing regime, particularly

with its ability to prosecute and convict money launderers. To create a more effective regime, Mexico should fully implement and improve its mechanisms for asset forfeiture; increase personnel responsible for the initiation, investigation, and prosecution of money laundering cases; control the bulk smuggling of currency across its borders; monitor remittance systems for possible exploitation; and improve the regulation of centros cambiarios. The GOM should also ensure that its newly-adopted counter-terrorist financing law is fully implemented.

## Moldova

Moldova is not considered an important regional financial center. The Government of Moldova (GOM) monitors money flows through right-bank Moldova (the territory it controls), but does not exercise control over the breakaway region of Transnistria. Transnistrian authorities do not submit to GOM financial controls and maintain an independent banking system not licensed by the National Bank of Moldova. Moldovan incomes are generally low. Criminal proceeds laundered in Moldova derive substantially from tax evasion, contraband smuggling, foreign criminal activity, and, to a lesser extent, domestic criminal activity and corruption. Money laundering proceeds are controlled by small, poorly-organized domestic criminal groups. These small groups are in turn supervised by larger and better-organized foreign crime syndicates from Russia, Ukraine, and Israel, among others.

Money laundering has occurred in the banking system and through exchange houses in Moldova, and in the offshore financial centers in Transnistria and throughout the region. The amount of money laundering occurring via alternative remittance systems is reportedly not significant. The number of financial crimes unrelated to money laundering, such as bank fraud, embezzlement, corruption, and forgery of bankcards, especially through international offshore zones, has decreased. During 2006, several cases involved bank fraud and the misuse of bankcards. Although the number of financial crimes has not increased, investigations have revealed a diversification of financial and economic-related crimes.

Although a significant black market exists in Moldova, especially smuggling of goods at the Moldovan-Ukrainian border alongside Transnistria, narcotics proceeds are not a significant funding source of this market. Contraband smuggling generates funds that are laundered through the banking system. Often funds are first laundered through Transnistrian banks, next transferred to Moldovan institutions, and then transferred to other countries.

Moldova is not considered an offshore financial center. The Moldovan financial system has 15 banks, including three foreign-owned banks that are regulated in the same manner as Moldovan commercial banks. Offshore banks are not permitted to operate in Moldova. Shell companies are not allowed by law, although they exist on a de facto basis. Nominee directors and trustees are not allowed. Internet gaming sites do exist, although no statistics are currently available on the number of sites in operation. Internet gaming is subject to the same regulations as domestic casinos. The Ministry of Finance currently licenses five casinos, although they are reportedly not well regulated or controlled.

Moldova currently has six free trade zones (FTZs). Certain free-trade zones are infrequently used. Goods from abroad are imported to the free economic zones and resold without payment of customs duties of the country of origin or of Moldova. The goods are then exported to other countries with documentation, indicating Moldovan origin. According to the Moldova's financial intelligence unit (FIU), the Service for Preventing and Combating Money Laundering and Terrorism Financing, no reports have been filed alleging that the free zones have been used in trade-based money laundering schemes or for terrorist financing. Supervision of the FTZs is conducted by a GOM agency, the Free Trade Zone Administration (FTZA). Companies operating in free-trade zones are also subject to inspections, controls, and investigations by inspectors from the Customs Service and the Center for Combating Economic Crime and Corruption (CCECC).

Money laundering is a separate criminal offense in the Moldovan Criminal Code, Art. 243, and under the Law on Preventing and Combating Money Laundering and Terrorism, No.190-XVI, passed on July 26, 2007. The legislation takes an "all serious crimes" approach. Serious crimes are defined as those punishable by a fine of 500 to 1,000 conventional units (U.S. $900 to $1,800) or by imprisonment of up to five years. The fine or imprisonment may be accompanied by a prohibition to hold certain positions or to practice a certain activity for a period of two to five years.

On April 10, 2007, President Vladimir Voronin proposed to the Moldovan Parliament draft amendments to the tax code and other financial regulations aimed at "liberalizing the economy." On April 27, the Parliament adopted these tax-code amendments intended to regulate Moldova's informal economy, forgive tax debts and stimulate investments. Some provisions of the financial package raised concerns as they could facilitate money laundering and terrorist financing. Of particular concern was a capital-amnesty provision allowing individuals and legal entities (corporations, partnerships, etc.) to legalize previously undeclared cash and noncash assets, including real estate and stocks. According to the proposed legislation, the GOM would encourage asset declaration by ensuring the confidentiality of all transactions and protecting filers from any future fiscal investigations. Additionally, those taking advantage of the amnesty would be under no obligation to declare the origins of their declared assets. The law also stipulated that transaction information could not be shared with the CCECC or the Moldovan Tax Inspectorate. Most worrisome, the legislation exempted declared assets from Moldova's fiscal, customs and current money laundering and terrorist financing legislation.

Following recommendations from the international community, on July 20, 2007, the Moldovan Parliament adopted Law 2298, a package of tax-code reforms, which included amendments to the capital-amnesty law. The amendment closed loopholes in the capital-amnesty law, eliminating explicitly the exemption of amnesty-related transactions from Moldova's anti-money laundering law. A week later, Parliament separately adopted the new anti-money laundering bill, the Law on Preventing and Combating Money Laundering and Terrorism. Since their passage, GOM authorities have issued numerous regulations, decisions, and laws that are related to the tax-amnesty/capital-legalization law and the new money laundering law. On August 15, 2007, the National Bank of Moldova issued two decisions focusing on the activity of financial institutions related to capital legalization and the transfer or export from the Republic of Moldova of legalized funds by individuals.

Article 12 of the Law on Preventing and Combating Money Laundering and Terrorism regulates the limitations of bank secrecy. Thus, information obtained from reporting entities can be used only with the purpose of preventing money laundering and terrorist financing. The forwarding of information regarding clients or ownership information to the CCECC, criminal investigative authorities, prosecutorial entities, or to the courts in an effort to prevent or combat money laundering activities is not classified as disclosure of commercial bank or professional secrets, as long as the forwarding of information is carried out in accordance with legal provisions.

All banks and nonbanking financial institutions are supervised and examined for compliance with anti-money laundering/counter-terrorist financing (AML/CTF) laws and regulations by the CCECC, which has the authority to investigate money laundering and terrorist financing. Under the Law on Preventing and Combating Money Laundering and Terrorism, the National Bank of Moldova (NBM) supervises banks, exchange houses, and representatives of foreign banks. Moreover, based on the July 2007 amendment of Law No. 192 from December 11, 1998, on the Securities Commission, three institutions dealing with oversight of financial markets—the National Commission on Securities, the Inspectorate for Supervision of Insurance Companies and Retirement Funds, and the National Service for Supervision of Citizen's Savings and Lending Associations—were merged into one agency, the National Commission on Financial Markets (NCFM). The NCFM's jurisdiction includes nonbanking financial entities, such as institutions issuing securities, investors, the National Bureau of Insurance of Vehicles of Moldova, members of saving and lending associations, and clients of micro-financing organizations. Additionally, the NCFM oversees professional participants in the nonbanking financial

sector that have license to carry out activities in the following fields: securities market, insurance market, micro-financing, private pension funds, mortgage organizations, and credit-history bureaus. The Licensing Chamber checks the compliance of companies applying for business licenses, and specifically oversees casinos and gambling facilities.

Banks, exchange houses, stock brokerages, casinos, insurance companies, lawyers, notaries, accountants, and lotteries and institutions organizing or displaying lotteries are required to know, record, and report the identity of customers engaging in significant transactions. The reporting entities are obligated to report suspicious transactions to the FIU within 24 hours. In addition, single transactions or multiple transactions undertaken in 30 calendar days that exceed MDL 500,000 (approximately U.S. $45,000) must be reported to the FIU. The Law on Preventing and Combating Money Laundering and Terrorism also requires that financial institutions maintain records and documentation of accounts account holders and basic documentation (including business correspondence) for a period of at least seven years after the termination of business relations or the closing of the account.

Moldova's FIU is a quasi-independent unit within the CCECC. Decree No. 111 of September 15, 2003, establishes the FIU as an administrative and analytical body that collects, maintains, and analyzes reports from reporting institutions. It also conducts criminal investigations and has regulatory authority to develop draft laws. The FIU is staffed with 14 inspectors. Although housed within the CCECC building, a separate locked door separates its offices from other CCECC employees. The heads of the FIU and the CCECC maintain that other CCECC employees have no access to records collected by the FIU. However, the leadership of the FIU is ultimately under the supervision of the director of the CCECC. While the CCECC budget covers the financial needs of the FIU, the FIU is also supported technically and financially by international organizations. The head of the FIU reports that the unit is adequately staffed, with low turnover, good working conditions and newly renovated offices. However, it analytical functions are limited without a database, which it currently cannot afford.

The CCECC and the FIU are the lead agencies responsible for investigating financial crimes, including money laundering. Other agencies that share jurisdiction over the investigation of financial crimes include the Prosecutor General's Office, the Ministry of Interior and the Customs Service. The Security and Intelligence Service (SIS) investigates terrorist financing. The FIU has formed a task force with the Prosecutor General's Office, the Ministry of the Interior (MOI), the Customs Service, the NBM, the National Securities Commission, the SIS, and the Ministry of Information Development to share information and discuss investigations. The FIU has signed interagency agreements with other law enforcement agencies and ministries with databases to exchange law-enforcement information.

In 2007, the FIU received reports on approximately 9 million financial transactions, of which 165,199 were considered suspicious. This number of suspicious transactions is misleading, however, since GOM officials categorize all transactions involving Transnistria as suspicious.

In 2007, the FIU initiated eleven criminal cases related to financial fraud; four cases carried money laundering charges. The FIU identified two major types of criminal activity in 2006 and during the first six months of 2007. In the first instance, criminals used financial transactions that appeared to be legitimate to launder or clean criminal proceeds. In the second instance, criminals used the FTZs to create illegal profits by reducing the value of imported goods. In 2007, the FIU imposed fines and sanctions totaling MDL 550,000 (approximately U.S. $49,600). The FIU reports that no arrests of individuals were conducted in 2006 or during the first six months of 2007 for money laundering violations. Late in 2007, a Moldovan court tried a criminal case charging the defendant with money laundering violations. The defendant was found guilty and sentenced to 15 years imprisonment. The FIU and CCECC have made no arrests nor pursued prosecutions involving terrorist financing.

Law No. 1569 of December 2002 on the transportation of currency stipulates that persons are obliged to report in writing to Moldovan customs officials the amount of currency that they are transporting when that amount exceeds 10,000 euros. If the amount of outbound currency is more than 10,000 euros, the carrier of the currency will have to report the outbound currency in a special declaration form provided by customs officials at the border. In addition to the special declaration, the currency carrier must provide documents detailing the source of the money. The carrier also must present a special permission for outbound cash currency transportation issued by a duly authorized bank or by the NBM. The Customs Service operates a special database that includes all declarations. The Customs Service shares the information in the database with other governmental agencies, including the FIU.

The Moldovan Criminal Code provides for the seizure and confiscation of assets related to all serious crimes, including terrorist financing. The provisions may be applied to goods belonging to persons who knowingly accepted things acquired illegally, even when the state declines to prosecute. However, it remains unclear whether asset forfeiture may be invoked against those unwittingly involved in or tied to an illegal activity. If it can be shown that the assets were used in the commission of a crime or result from a crime, they can be confiscated. Legitimate businesses can be seized if they were used to launder drug money, support terrorist activity, or are otherwise related to other criminal proceeds. The Criminal Code allows for civil as well as criminal forfeiture.

The Prosecutor General's Office has expressed its willingness to pursue an initiative to amend the Constitution to allow a more effective use of asset forfeiture. The Constitution currently incorporates a presumption that any property owned by an individual was legally acquired. This presumption has acted to inhibit the use of the existing asset forfeiture laws. Subsequent to a constitutional amendment, the Prosecutor General's Office plans generally to update the laws governing the identification of criminal assets and the use of asset forfeiture.

The FIU, CCECC, Tax Inspectorate, Customs Service and prosecutor's offices to the extent of their jurisdiction are responsible for tracing, seizing and freezing assets. Assets seized by law enforcement are incorporated into the state budget, not a separate fund. In 2007, issued decisions freezing and seizing assets totaling MDL 14.8 million (approximately U.S. $1.3 million).

The banking community generally cooperates with enforcement efforts of the FIU and the CCECC to trace funds and seize or freeze bank accounts. However, the GOM currently lacks adequate resources, training, and experience to trace and seize assets effectively. The GOM does not have a national system for freezing terrorist assets. The GOM has no separate law providing for the sharing with other countries of assets seized from narcotics and other serious crimes. However, nothing in the current legal structure would prohibit such activity.

Article 279 of the Moldovan Criminal Code criminalizes terrorist financing. It is defined as a "serious crime." Moldova regulates efforts to combat terrorist financing in the Law on Combating Terrorism, enacted on November 12, 2001. Article 2 defines terrorist financing, and Article 8/1 authorizes suspension of terrorist and related financial operations. This statute is separate from the aforementioned money laundering law, which contains other relevant provisions.

In 2007, the CCECC issued a decree on actions to be taken to enforce the provisions of the Law on Preventing and Combating Money Laundering and Terrorism. The CCECC decree listed groups worthy of particular focus given possible money laundering or terrorist financing concerns. These groups included countries that may produce narcotics; countries that do not have legal provisions against money laundering and terrorist financing; countries with a high crime rate and corruption; countries operating offshore centers; and persons, groups, and entities identified as participating in terrorist activities. The decree was developed on the basis of Moldova's national interests and U.S. and UN lists of designated terrorists. Currently, the Moldovan authorities have not frozen, seized, or forfeited assets related to terrorism and terrorist financing. Reportedly, no indigenous alternative

remittance systems exist in Moldova, although the use of cash couriers is common. No special measures have been taken to investigate misuse of charitable or nonprofit entities.

In December 2006, the GOM signed a $24.7 million Threshold Country Program with the Millennium Challenge Corporation that focuses on anti-corruption measures. The GOM requested funding to address areas of persistent corruption including the judiciary, health care system, tax, customs and law enforcement. Moldova is listed as 111 out of 180 countries in Transparency International's 2007 Corruption Perception Index.

The GOM has no bilateral agreement with the United States for the exchange of information regarding money laundering, terrorism, or terrorist financing investigations and proceedings. However, Moldovan authorities continue to solicit USG assistance on individual cases and cooperate with U.S. law enforcement personnel when presented with requests for information or assistance. The FIU has entered into bilateral agreements to exchange information with financial intelligence units of Albania, Belarus, Bulgaria, Croatia, Estonia, Georgia, Indonesia, Korea, Lebanon, Lithuania, Macedonia, Romania, Russia, and Ukraine.

Moldova is a party to the 1988 UN Drug Convention, the International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. On October 1, 2007, the GOM ratified the UN Convention against Corruption. Moldova has signed an agreement with CIS member states for the exchange of information on criminal matters, including money laundering. In 2004, the CCECC was accepted as an observer at the Eurasian Group on Combating Money Laundering. Moldova is a member of the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). The FIU is currently pursuing membership in the Egmont Group of financial intelligence units.

The Government of Moldova should continue to enhance its existing anti-money laundering and counter-terrorist financing regime. The GOM should ensure that the FIU and law enforcement agencies have sufficient resources, training, and tools to adequately analyze and investigate suspected cases of money laundering and terrorist financing. Moldova should improve the mechanisms for sharing information and forfeiting assets. Border enforcement and antismuggling enforcement should be priorities. The GOM should continue the momentum of its anticorruption efforts.

## Monaco

The second-smallest country in Europe, the Principality of Monaco is known for its tradition of bank secrecy, network of casinos, and favorable tax regime. Money laundering offenses relate mainly to offenses committed abroad. Russian organized crime and the Italian Mafia reportedly have laundered money in Monaco. The Principality is also reported not to face the ordinary forms of organized crime. Existing crime does not seem to generate significant illegal proceeds, with the exception of fraud and offenses under the "Law on Checks." Monaco remains on an Organization for Economic Cooperation and Development (OECD) list of so-called "noncooperative" countries in terms of provision of tax information.

Monaco has a population of approximately 32,000, of which fewer than 7,000 are Monegasque nationals. Monaco's approximately 60 banks and financial institutions hold more than 300,000 accounts and manage total assets of about 70 billion euros (approximately U.S. $102.8 billion). Approximately 85 percent of the banking customers are nonresident. In 2005, the financial sector represented 15 percent of Monaco's economic activity. The high prices for land throughout the Principality result in a real estate sector of considerable import. There are five casinos run by the Société des Bains de Mer, in which the state holds a majority interest.

Monaco's banking sector is linked to the French banking sector through the Franco-Monegasque Exchange Control Convention, signed in 1945 and supplemented periodically, most recently in 2001.

Through this convention, Monaco operates under the banking legislation and regulations issued by the French Banking and Financial Regulations Committee, including Article 57 of France's 1984 law regarding banking secrecy. The majority of entities in Monaco's banking sector concentrate on portfolio management and private banking. Subsidiaries of foreign banks operating in Monaco may withhold customer information from their parent banks.

Banking laws do not allow anonymous accounts, but Monaco does permit the existence of alias accounts, which allow account owners to use pseudonyms in lieu of their real names. Cashiers do not know the clients, but the banks know the identities of the customers and retain client identification information. Article 8 of Sovereign Order 632 of August 2006 clarifies the circumstances under which pseudonyms can be used by banks.

Prior approval is required to engage in any economic activity in Monaco, regardless of its nature. The Monegasque authorities issue approvals based on the type of business to be engaged in, the location, and the length of time authorized. This approval is personal and may not be re-assigned. Any change in the terms requires the issuance of a new approval.

Although the French Banking Commission supervises Monegasque credit institutions, Monaco shoulders the responsibility for legislating and enforcing measures to counter money laundering and terrorist financing. The Finance Counselor, located within the Government Council, is responsible for anti-money laundering and counter-terrorist financing (AML/CTF) implementation and policy.

Money laundering in Monaco is a crime under Act 1.162 of July 7, 1993, "On the Participation of Financial Institutions in the Fight against Money Laundering," and Section 218-3 of the Criminal Code, amended by Act 1.253 of July 12, 2002, "Relating to the Participation of Financial Undertakings in Countering Money Laundering and the Financing of Terrorism." On November 9, 2006, Section 218-3 of the Criminal Code was modified to adopt an "all crimes" approach to money laundering.

Monaco's anti-money laundering legislation, as amended, requires banks, insurance companies, stockbrokers, corporate service providers, portfolio managers, some trustees, and institutions within the offshore sector to report suspicious transactions to Monaco's financial intelligence unit (FIU), and to disclose the identities of those involved. Casino operators must alert the government of suspicious gambling payments possibly derived from drug trafficking or organized crime. The law imposes a five to ten-year jail sentence for anyone convicted of using illicit funds to purchase property, which itself is subject to confiscation. Act 1.162, as amended, institutes procedural requirements regarding internal compliance, client identification, and retention and maintenance of records. Sovereign Order 16.615 of January 2005 and Sovereign Order 631 of August 2006 mandate additional customer identification measures. Designated nonfinancial businesses and professions, such as lawyers, notaries, accountants, real estate brokers, and dealers in precious metals and stones, are not subject to reporting or record-keeping requirements.

Offshore companies are subject to the same due diligence and suspicious reporting obligations as banking institutions, and Monegasque authorities conduct on-site audits. Act 1.253 strengthens the "know your client" obligations for casinos and obliges companies responsible for the management and administration of foreign entities not only to report suspicions to Monaco's FIU, but also to implement internal AML/CTF procedures. The FIU monitors these activities.

Monaco's FIU, the Service d'Information et de Controle sur les Circuits Financiers (SICCFIN), receives suspicious transaction reports, analyzes them, and forwards them to the prosecutor when they relate to drug trafficking, organized crime, terrorism, terrorist organizations, or the funding thereof. SICCFIN also supervises the implementation of AML legislation. Under Article 4 of Law 1.162, SICCFIN may suspend a transaction for twelve hours and advise the judicial authorities to investigate. SICCFIN has received between 200 and 400 suspicious transaction reports (STRs) annually from 2000

to 2006. In 2006, SICCFIN received 395 STRs, about 50 percent of which were submitted by banks and other financial institutions. SICCFIN received 60 requests for financial information from other FIUs in 2006. No statistics are currently available on the number of reports or requests received by SICCFIN in 2007.

Investigations and prosecutions are handled by the two-officer Money Laundering Unit (Unite de Lutte au Blanchiment) within the police. The Organized Crime Group (Groupe de Repression du Banditisme) may also handle cases. Seven police officers have been designated to work on money laundering cases. Four prosecutions for money laundering have taken place in Monaco, which have resulted in three convictions.

Monaco's legislation allows for the confiscation of property of illicit origin as well as a percentage of co-mingled illegally acquired and legitimate property. Authorities must obtain a court order to confiscate assets. Confiscation of property related to money laundering is restricted to the offenses listed in the Criminal Code. Authorities have seized assets exceeding 11.7 million euros (approximately U.S. $17 million) in value as of year-end 2006. Monaco and the United States signed a seized asset sharing agreement in March 2007.

In July and August 2002, the Government of Monaco (GOM) passed Act 1.253 and promulgated two Sovereign Orders intended to implement United Nations Security Council Resolution 1373 by outlawing terrorism and its financing. Monaco passed additional Sovereign Orders in April and August of that year, importing into Monegasque law the obligations of the UN International Convention for the Suppression of the Financing of Terrorism. In 2006, Monaco further amended domestic law to implement these obligations.

The Securities Regulatory Commissions of Monaco and France signed a memorandum of understanding (MOU) in March 2002 on the sharing of information between the two bodies. The GOM considers this MOU an important tool to combat financial crime, particularly money laundering. SICCFIN has signed information exchange agreements with over 20 foreign FIUs. In March 2007, Monaco ratified the European Convention on Mutual Assistance in Criminal Matters. Monaco has neither signed nor ratified the European Convention on Extradition, although it has concluded 15 extradition treaties with various countries. To date, there have been no extraditions on the grounds of money laundering, although the GOM has extradited criminals guilty of other offenses, mainly to Russia.

Monaco is a member of the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). SICCFIN is a member of the Egmont Group of financial intelligence units. Monaco 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 GOM has neither signed nor ratified the UN Convention against Corruption.

The Government of Monaco should amend its legislation to implement full corporate criminal liability. The Principality should continue to enhance its anti-money laundering and confiscation regimes by fully applying its AML/CTF reporting, customer identification, and record-keeping requirements to all trustees and gaming houses. The GOM should also consider extending AML/CTF regulations to designated nonfinancial businesses and professions. SICCFIN should have the authority to forward reports and disseminate information to law enforcement even when the report or information obtained does not relate specifically to drug trafficking, organized crime, or terrorist activity or financing. Monaco should become a party to the UN Convention against Corruption.

## Morocco

Morocco is not a regional financial center, but money laundering is a concern due to its narcotics trade, vast informal sector, trafficking in persons, and large level of remittances from Moroccans living abroad. According to the 2007 World Drug Report by the United Nations Office on Drugs and Crime (UNODC), Morocco remains a principal producer and exporter of cannabis, while credible estimates of Morocco's informal sector range between 17 and 40 percent of GDP. In 2006, remittances from Moroccans living abroad valued $5.4 billion, approximately nine percent of GDP. Although the true extent of the money laundering problem in the country is unknown, conditions exist for it to occur. In the past few years, the Kingdom of Morocco has taken a series of steps to address the problem, most notably the enactment of a comprehensive anti-money laundering (AML) bill in May 2007 and the establishment of a Financial Intelligence Unit, expected to become operational in Rabat in early 2008.

The predominant use of cash, informal value transfer systems and remittances from abroad all help fuel Morocco's informal sector. Bulk cash smuggling is also a problem. There are unverified reports of trade-based money laundering, including under-and over-invoicing and the purchase of smuggled goods. Most businesses are cash-based with little invoicing or paper trail. Cash-based transactions in connection with cannabis trafficking are of particular concern. According to the UNODC, Morocco remains the world's principal producer of cannabis, with revenues estimated at over $13 billion annually. While some of the narcotics proceeds are laundered in Morocco, most proceeds are thought to be laundered in Europe.

Unregulated money exchanges remain a problem in Morocco and were a prime impetus for Morocco's recent AML legislation. Although the legislation targets previously unregulated cash transfers, the country's vast informal sector creates conditions for this practice to continue. The Moroccan financial sector is underdeveloped, consisting of 16 banks, five government-owned specialized financial institutions, approximately 30 credit agencies, and 12 leasing companies. The monetary authorities in Morocco are the Ministry of Finance and the Central Bank—Bank Al Maghrib—that monitors and regulates the banking system. A separate Foreign Exchange Office regulates international transactions.

Since 2003, Morocco has taken a series of steps to tighten its AML controls. In December 2003, the Central Bank issued Memorandum No. 36, in advance of pending AML legislation that instructed banks and other financial institutions under its control to conduct internal analysis and investigations into financial transactions. The measures called for the reporting of suspicious transactions, retention of suspicious activity reports, and mandated "know your customer" procedures. In 2007, Morocco's AML efforts took a significant step forward with parliamentary passage and promulgation of a comprehensive AML law, which draws heavily from Financial Action Task Force (FATF) recommendations. The law requires the reporting of suspicious financial transactions by all responsible parties, both public and private, who in the exercise of their work, carry out or advise on the movement of funds possibly related to drug trafficking, human trafficking, arms trafficking, corruption, terrorism, tax evasion, or forgery. There were no prosecutions for money laundering in Morocco in 2007.

Morocco has a free trade zone in Tangier, with customs exemptions for goods manufactured in the zone for export abroad. There have been no reports of trade-based money laundering schemes or terrorist financing activities using the Tangier free zone or the zone's offshore banks, which are regulated by an interagency commission chaired by the Ministry of Finance.

While there have been no verified reports of international or domestic terrorist networks using the Moroccan narcotics trade to finance terrorist organizations and operations in Morocco, investigations into the Ansar Al Mahdi and Al Qaeda in the Islamic Maghreb (AQIM) terrorist organizations are ongoing. At least two suspects arrested as part of the Ansar Al Mahdi cell were accused of providing financing to the cell.

Morocco has a relatively effective system for disseminating U.S. Government (USG) and United Nations Security Council Resolution (UNSCR) terrorist freeze lists to the financial sector and law enforcement. Morocco has provided detailed and timely reports requested by the UNSCR 1267 Sanctions Committee and some accounts have been administratively frozen (based on the U.S. list of Specially Designated Global Terrorists, designated pursuant to Executive Order 13224). In 1993, a mutual legal assistance treaty between Morocco and the United States entered into force.

Morocco is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of Financing of Terrorism, and the UN Convention against Transnational Organized Crime. On May 9, 2007, Morocco ratified the UN Convention against Corruption. Morocco is ranked 72 out of 179 countries surveyed in Transparency International's 2007 International Corruption Perception Index. Morocco has ratified or acceded to 11 of the 12 UN and international conventions and treaties related to counterterrorism. Morocco is a charter member of the Middle East and North Africa Financial Action Task Force (MENAFATF).

In June 2003, Morocco adopted a comprehensive counterterrorism bill. This bill provided the legal basis for lifting bank secrecy to obtain information on suspected terrorists, allowed suspect accounts to be frozen, and permitted the prosecution of terrorist finance-related crimes. The law also provided for the seizure and confiscation of terrorist assets, and called for increased international cooperation with regard to foreign requests for freezing assets of suspected terrorist entities. The counterterrorism law brought Morocco into compliance with UNSCR 1373 requirements for the criminalization of the financing of terrorism. Other AML controls include legislation prohibiting anonymous bank accounts and foreign currency controls that require declarations to be filed when transporting currency across the border.

The Government of Morocco should continue to implement anti-money laundering/counter-terrorist financing (AML/CTF) programs and policies that adhere to world standards, including a viable FIU that receives, analyzes, and disseminates financial intelligence. The informal economy is very significant in Morocco and authorities are likely to face major challenges as the new AML regime is implemented. Police and customs authorities, in particular, should receive training on recognizing money laundering methodologies, including trade-based laundering and informal value transfer systems.

## The Netherlands

The Netherlands is a major financial center and an attractive venue for the laundering of funds generated from a variety of illicit activities. Activities involving money laundering are often related to the sale of heroin, cocaine, cannabis, or synthetic and designer drugs (such as ecstasy). As a major financial center, several Dutch financial institutions engage in international business transactions involving large amounts of United States currency. There are, however, no indications that significant amounts of U.S. dollar transactions conducted by financial institutions in the Netherlands stem from illicit activity. Activities involving financial fraud are believed to generate a considerable portion of domestic money laundering. A recent report by the University of Utrecht commissioned by the Ministry of Finance has found that much of the money laundered in the Netherlands originates abroad, but did not find evidence that it is predominantly owned by major drug cartels and other international criminal organizations. There are no indications of syndicate-type structures in organized crime or money laundering, and there is virtually no black market for smuggled goods in the Netherlands. Although under the Schengen Accord there are no formal controls on national borders within the EU, the Dutch authorities run special operations in its border areas with Germany and Belgium to keep smuggling to a minimum. Reportedly, money laundering amounts to 18.5 billion euros (approximately U.S. $27.14 billion) annually, or five percent of the Dutch GDP. The Netherlands is not an offshore financial center nor are there any free trade zones in the Netherlands.

In 1994, the Government of the Netherlands (GON) criminalized money laundering related to all crimes. In December 2001, the GON enacted legislation specifically criminalizing facilitating, encouraging, or engaging in money laundering. This eases the public prosecutor's burden of proof regarding the criminal origins of proceeds: under the law, the public prosecutor needs only to prove that the proceeds "apparently" originated from a crime. Self-laundering is also covered. In two cases in 2004 and 2005, the Dutch Supreme Court confirmed the broad application of the money laundering provisions by stating that the public prosecutor does not need to prove the exact origin of laundered proceeds for conviction, and that the general criminal origin as well as the knowledge of the perpetrator may be deduced from objective circumstances.

The Netherlands has an "all offenses" regime for predicate offenses of money laundering. The penalty for "deliberate acts" of money laundering is a maximum of four years' imprisonment and a maximum fine of 45,000 euros (approximately U.S. $66,000), while "liable acts" of money laundering (by people who do not know first-hand of the criminal nature of the origin of the money, but should have reason to suspect it) are subject to a maximum imprisonment of one year and a fine no greater than 45,000 euros (approximately U.S. $66,000). Habitual money launderers may be punished with a maximum imprisonment of six years and a maximum fine of 45,000 euros (approximately U.S. $66,000), and those convicted may also have their professional licenses revoked. In addition to criminal prosecution for money laundering offenses, money laundering suspects can also be charged with participation in a criminal organization (Article 140 of the Penal Code), violations of the financial regulatory acts, violations of the Sanctions Act, or noncompliance with the obligation to declare unusual transactions according to the Economic Offenses Act.

The Netherlands has comprehensive anti-money laundering (AML) legislation. The Services Identification Act and the Disclosure Act set forth identification and reporting requirements. All financial institutions in the Netherlands, including banks, bureaux de change, casinos, life insurance companies, securities firms, stock brokers, and credit card companies, are required to report cash transactions over certain thresholds (varying from 2,500 to 15,000 euros or approximately U.S. $3,670 to $21,000), as well as any less substantial transaction that appears unusual (applying a broader standard than "suspicious" transactions) to the Netherlands' financial intelligence unit (FIU-the Netherlands). Reporting requirements have been expanded to include financing companies, commercial dealers of high-value goods, notaries, lawyers, real estate agents/intermediaries, accountants, business economic consultants, independent legal advisers, tax advisors, trust companies and other providers of trust-related services. In 2007, the notary sector supervisor, BFT, reported that seven notaries allegedly violated AML rules but due to client confidentiality, the names of the notary firms were not released, . Reportedly, the agencies received cash payments above the reporting threshold and failed to report, and facilitated quick transfers of ownership for property. BFT investigators found 192 suspicious cases in 2004 and 2005, and a similar number in 2006 and 2007. The BFT has requested amended legislation.

Since 2005, the GON has implemented measures to enhance the effectiveness of its AML regime. A November 2005 National Directive on money laundering crimes mandates a financial investigation in every serious crime case, sets guidelines for determining when to prosecute for money laundering and provides technical explanations of money laundering offenses, case law, and the use of financial intelligence. Revised indicators determine when an unusual transaction report must be filed. The indicators reflect a partial shift from a rule-based to a risk-based system and are aimed at reducing the administrative costs of reporting unusual transactions without limiting the preventive nature of the reporting system. Amendments to the Services Identification Act and Disclosure Act expand supervision authority and institute punitive damages. The revised legislation, which became effective on May 1, 2006, also incorporates a terrorist-financing indicator in the reporting system.

Financial institutions are required by law to maintain records necessary to reconstruct financial transactions for five years after termination of the relationship. There are no secrecy laws or fiscal

regulations that prohibit Dutch banks from disclosing client and owner information to bank supervisors, law enforcement officials, or tax authorities. All institutions under the reporting and identification acts, and their employees, are specifically protected by law from criminal or civil liability related to cooperation with law enforcement or bank supervisory authorities. The Money Transfer and Exchange Offices Act, passed in June 2001, requires money transfer offices, as well as exchange offices, to obtain a permit to operate, and subjects them to supervision by the Central Bank. Every money transfer client must be identified and all transactions totaling more than 2,000 euros (approximately U.S. $2,935) must be reported to the FIU. Sharing of information by Dutch supervisors does not require formal agreements or memoranda of understanding (MOUs).

The FIU for the Netherlands is a hybrid administrative-law enforcement unit that in 2006 combined the original, administrative FIU MOT (Meldpunt Ongebruikelijke Transacties, or in English the Office for the Disclosure of Unusual Transactions) with its police counterpart, the Office of Operational Support of the National Public Prosecutor (BLOM). When MOT, established in 1994, and BLOM merged, the resulting entity was integrated within the National Police (KLPD). The new unit, FIU-the Netherlands, not only provides an administrative function that receives, analyzes, and disseminates the unusual and currency transaction reports filed by banks, financial institutions and other reporting entities, but it also provides a police function that serves as a point of contact for law enforcement. It forwards suspicious transaction reports (STRs) with preliminary investigative information to the Police Investigation Service. Over the last five years, the MOT and the BLOM have responded to international requests for financial and law enforcement information, including those from counterpart FIUs, so this merger has not changed the nature of the Dutch reporting system with respect to international cooperation. FIU-the Netherlands is a member of the Egmont Group.

Obliged entities that fail to file reports with the FIU-the Netherlands can be prosecuted in two ways. One of the four supervisory bodies, depending on the entity, may impose an administrative fine of up to 32,670 euros (approximately U.S. $47,905), depending on the size of the entity. The Dutch Tax Administration supervises commercial dealers; the Bureau Financieel Toezicht (BFT or Office for Financial Oversight) supervises notaries, lawyers, real estate agents, and accountants; de Nederlandsche Bank (Dutch Central Bank) supervises trust companies, casinos, banks, bureaux de change, and insurance companies; and the Authority for Financial Markets supervises clearinghouses, brokers, and securities firms. The public prosecutor may fine nonreporting entities 11,250 euros (approximately $16,495), or charge individuals failing to report with prison terms of up to two years. Under the Services Identification Act, those subject to reporting obligations must identify their clients, including the identity of beneficial owners, either at the time of the transaction or prior to the transaction, before providing financial services.

The FIU receives every unusual transaction report electronically through its secure website. In 2005, the FIU-the Netherlands received 181,623 reports and forwarded 38,481, totaling over 1.1 billion euros (approximately U.S. $1.6 billion), to enforcement agencies such as the police, fiscal police, and public prosecutor. In 2006, the FIU-the Netherlands received 172,865 unusual transaction reports and forwarded 34,531, totaling over 9.2 billion euros (approximately U.S. $13.5 billion) to enforcement agencies as suspicious transactions for further investigation. The average amount reported was 26,870 euros (approximately U.S. $39,400) in 2006, a decrease from the 28,945 euros (approximately U.S. $42,440) average reported in 2005. Approximately 89 percent of the transactions are in euros, 8 percent are in other European currency (of which 5 percent are in English Pounds) and finally 3 percent of the transactions are in U.S. dollars.

To facilitate the forwarding of STRs, the FIU created an electronic network called Intranet Suspicious Transactions (IST). Fully automatic matches of data from the police databases are included with the unusual transaction reports forwarded to enforcement agencies. On January 1, 2003, the former MOT and BLOM organizations together created a special unit (the MBA unit) to analyze data generated from the IST. Under the new FIU-the Netherlands structure, the MBA continues to analyze IST data

and forwards reports to the police. Since the money laundering detection system also covers areas outside the financial sector, the system is used for detecting and tracing terrorist financing activity. The FIU-the Netherlands provides the AML division of Europol with suspicious transaction reports, and Europol applies the same analysis tools as the FIU.

Current legislation requires Customs authorities to report unusual transactions to the FIU-the Netherlands. On June 15, 2007, EU regulation 1889/2005 on Liquid Assets Control introduced a currency declaration requirement for amounts valued over 10,000 euros for travelers entering and leaving Schengen-agreement countries. Travelers crossing Dutch borders must complete a declaration form. The Dutch use specially trained dogs at ports and airports to identify cash smugglers in 2006 finding four million euros (approximately $5.9 million) in passenger luggage at Schiphol airport.

The Netherlands has enacted legislation governing asset forfeiture. The 1992 Asset Seizure and Confiscation Act enables authorities to confiscate assets that are illicitly obtained or otherwise connected to criminal acts. The GON amended the legislation in 2003 to improve and strengthen the options for identifying, freezing, and seizing criminal assets. The police and several special investigation services are responsible for enforcement in this area. These entities have adequate powers and resources to trace and seize assets. All law enforcement investigations into serious crime may integrate asset seizure.

Authorities may seize any tangible assets, such as real estate or other conveyances that were purchased directly with proceeds tracked to illegal activities. Both moveable property and claims are subject to confiscation. Assets can be seized as a value-based confiscation. Legislation defines property for the purpose of confiscation as "any object and any property right" and provides for the seizure of additional assets controlled by a drug trafficker. Proceeds from narcotics asset seizures and forfeitures are deposited in the general fund of the Ministry of Finance.

To facilitate the confiscation of criminal assets, the GON has instituted special court procedures that enable law enforcement to continue financial investigations to prepare confiscation orders after the underlying crimes have been successfully adjudicated. All police and investigative services in the field of organized crime rely on the real time assistance of financial detectives and accountants, as well as on the assistance of the Proceeds of Crime Office (BOOM), a special bureau advising the Office of the Public Prosecutor in international and complex seizure and confiscation cases. To further international cooperation in this area, BOOM played a leading role in the creation of an informal international network of asset recovery specialists aiming to exchange information and share expertise. Known as the Camden Asset Recovery Network (CARIN), this network was established in The Hague in September 2004. .

Statistics provided by the Office of the Public Prosecutor show that the assets seized in 2006 amounted to 17 million euros (approximately U.S. $24.9 million). This compares with 11 million euros in 2005 and 11 million euros in 2004 (approximately U.S. $14.5 million and U.S. $13 million respectively, based on the exchange rates at the time). The United States and the Netherlands have had an asset-sharing agreement in place since 1994. The Netherlands also has an asset-sharing treaty with the United Kingdom, and an agreement with Luxembourg.

In June 2004, the Minister of Justice sent an evaluation study to the Parliament on specific problems authorities encountered with asset forfeiture in large, complex cases. In response to this report, the GON announced several measures to improve the effectiveness of asset seizure enforcement, including steps to increase expertise in the financial and economic field, assign extra public prosecutors to improve the coordination and handling of large, complex cases, and establish a specific asset forfeiture fund. The Office of the Public Prosecutor designed a centralized approach for large confiscation cases and a more flexible approach for handling smaller cases. The improvements took effect in 2006 and have significantly increased BOOM's capacity to handle asset forfeiture cases.

Terrorist financing is a crime in the Netherlands. In August 2004, the Act on Terrorist Crimes, implementing the 2002 EU framework decision on combating terrorism, became effective. The Act makes recruitment for jihad, and conspiracy to commit a terrorist act, criminal offenses. In 2004, the government created a National Counterterrorism Coordinator's Office to streamline and enhance Dutch counterterrorism efforts.

UN resolutions and EU regulations form a direct part of the national legislation on sanctions in the Netherlands. The "Sanction Provision for the Duty to Report on Terrorism," passed in 1977, was amended in June 2002 to implement European Union (EU) Regulation 2580/2001. United Nations Security Council Resolution (UNSCR) 1373 is implemented through Council Regulation 2580/01; listing is through the EU Clearinghouse process. The ministerial decree provides authority to the Netherlands to identify, freeze, and seize terrorist finance assets. The decree also requires financial institutions to report to the FIU all transactions (actually carried out or intended) involving persons, groups, and entities that have been linked, either domestically or internationally, with terrorism. Any terrorist crime automatically qualifies as a predicate offense under the Netherlands "all offenses" regime for predicate offenses of money laundering. Involvement in financial transactions with suspected terrorists and terrorist organizations listed on the United Nations (UN) 1267 Sanctions Committee's consolidated list or designated by the EU has been made a criminal offense. UNSCR 1267/1390 is implemented through Council Regulation 881/02. Sanctions Law 1977 also addresses this requirement parallel to the regulation in the Netherlands. The Dutch have taken steps to freeze the assets of individuals and groups included on the UNSCR 1267 Sanctions Committee's consolidated list.

The Netherlands does not require a collective EU decision to identify and freeze assets suspected of being linked to terrorism nationally. In these cases, the Minister of Foreign Affairs and the Minister of Finance make the decision to execute the asset freeze. Decisions take place within three days after a target is identified. Authorities have used this instrument several times in recent years. In three cases, national action followed the actions taking place on the EU level. In one case, the entity was included on the UN 1267 list and thus included in the list that circulated pursuant to EU regulation 2002/881. In two other cases, the Netherlands successfully nominated the entity/individual for inclusion on the autonomous EU list that is compiled pursuant to Common Position 2001/931.

The 2004 Act on Terrorist Offenses introduced Article 140A of the Criminal Code, which criminalizes participation in a terrorist organization, and defines participation as membership or providing provision of monetary or other material support. Article 140A carries a maximum penalty of fifteen years' imprisonment for participation in, and life imprisonment for leadership of, a terrorist organization. Nine individuals were convicted in March 2006 on charges of membership in a terrorist organization. Legislation expanding the use of special investigative techniques was enacted in February 2007.

Unusual transaction reports by the financial sector act as the first step against the abuse of religious organizations, foundations and charitable institutions for terrorist financing. No individual or legal entity using the financial system (including churches and other religious institutions) is exempt from the client identification requirement. Financial institutions must also inquire about the identity of the ultimate beneficial owners. The second step, provided by Dutch civil law, requires registration of all active foundations with the Chambers of Commerce. Each foundation's formal statutes (creation of the foundation must be certified by a notary of law) must be submitted to the Chambers. Charitable institutions also register with, and report to, the tax authorities to qualify for favorable tax treatment. Approximately 15,000 organizations (and their managements) are registered in this way. The organizations must file their statutes, showing their purpose and mode of operations, and submit annual reports. Samples are taken for auditing. Finally, many Dutch charities are registered with or monitored by private "watchdog" organizations or self-regulatory bodies, the most important of which is the Central Bureau for Fund Raising. In April 2005, the GON approved a plan to improve Dutch

efforts to fight fraud, money laundering, and terrorist financing by replacing the current initial screening of founders of private and public-limited partnerships and foundations with an ongoing screening system. The GON aimed to introduce the new system in 2007.

Certain groups of immigrants use informal banks to send money to their relatives in their countries of origin. However, indicators point to the misuse of these informal banks for criminal purposes, including a small number of informal bankers deliberately engaging in money laundering transactions and cross-border transfers of criminal money. Initial research by the Dutch police and Internal Revenue Service and Economic Control Service (FIOD/ECD) indicates that the number of informal banks and hawaladars in the Netherlands is rising. The Dutch Government plans to implement improved procedures for tracing and prosecuting unlicensed informal or hawala-type activity, with the Dutch Central Bank, FIOD/ECD, the Financial Expertise Center, and the Police playing a coordinating and central role. The Dutch Finance Ministry has participated in a World Bank-initiated international survey on money flows by immigrants to their native countries, with a focus on relations between the Netherlands and Suriname. The Dutch Central Bank has initiated a study into the number of informal banking institutions in the Netherlands. In Amsterdam, a special police unit has been investigating underground bankers. These investigations have resulted in the disruption of three major underground banking schemes.

The Netherlands is in compliance with all FATF Recommendations, with respect to both legislation and enforcement. The Netherlands also complies with the Second EU Money Laundering Directive and plans to implement the Third EU Money Laundering Directive through the adoption of a new act on combating money laundering and terrorist financing that will enter into force in 2008.

The United States enjoys good cooperation with the Netherlands in fighting international crime, including money laundering. In September 2004, the United States and the Netherlands signed bilateral implementing instruments for the U.S.-EU mutual legal assistance and extradition treaties; the agreements have not yet been ratified. One provision of the U.S.-EU legal assistance agreement would facilitate the exchange of information on bank accounts. In 2007, the Dutch Ministry of Justice and the Dutch National Police began working two operational money laundering initiatives with U.S. law enforcement authorities in the Netherlands. This is the first time that such operations have been attempted in the Netherlands.

The FIU supervised the PHARE Project for the European Union. The PHARE Project was the European Commission's Anti-Money Laundering Project for Economic Reconstruction Assistance and provided support to Central and Eastern European countries in the development and/or improvement of AML regulations. When the PHARE project concluded in December 2003, the FIU moved forward with the development of the FIU.NET Project, (an electronic exchange of current information between European FIUs by means of a secure intranet), which the FIU continues to use.

The Netherlands is a member of the Financial Action Task Force and the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). The Netherlands was a founding member of the CARIN asset-recovery network, and participates in the Caribbean Financial Action Task Force as a Cooperating and Supporting Nation. As a member of the Egmont Group, the FIU has established close links with the U.S Treasury's FinCEN as well as with other Egmont members, and is involved in efforts to expand international cooperation. The Netherlands is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Corruption, and the UN Convention against Transnational Organized Crime.

The Netherlands should continue its shift to the risk-based approach throughout its regulatory and AML/CTF regime, as well as proceed with enacting its new AML/CTF legislation. The GON should continue with its plans implementing a screening system for private and public-limited partnerships, including attendant requirements for all charities to register with a supervisory state or state-

sanctioned body. The Netherlands should obtain statistics and examine the progress that has been achieved since the improvements in the asset forfeiture regime have been implemented. The GON should devote more resources toward getting better data and a better understanding of alternate remittance systems in the Netherlands, and channel more investigative resources toward tracing informal bank systems.

## Netherlands Antilles

The Netherlands Antilles is comprised of the islands of Curacao, Bonaire, Dutch Sint Maarten, Saba, and Sint Eustatius. Though a part of the Kingdom of the Netherlands, the Netherlands Antilles has autonomous control over its internal affairs. The Government of the Netherlands Antilles (GONA) is located in Willemstad, the capital of Curacao, which is also the financial center for the five islands. A significant offshore sector and loosely regulated free trade zones, as well as narcotics trafficking and a lack of border control between Sint Maarten (the Dutch side of the island) and St. Martin (the French side), create opportunities for money launderers in the Netherlands Antilles.

The Netherlands Antilles' banking sector consists of seven local general banks, 14 investment institutions, one subsidiary of a foreign general banks, two branches of foreign general banks, 12 credit unions, six specialized credit unions, one savings bank, four savings and credit funds, 15 consolidated international banks, 18 nonconsolidated international banks, and 22 pension funds. The laws and regulations on bank supervision provide that international banks must have a physical presence and maintain records on the island. There are multiple insurance companies, including three subsidiaries of foreign life insurance companies, seven branches of foreign life insurance companies, six subsidiaries of foreign nonlife insurance companies, six branches of foreign insurance companies, and six independent insurance companies. In addition, there are two captive life insurance companies, 13 captive nonlife insurance companies, four professional reinsurance companies, and one other health insurance company.

The Netherlands Antilles has an offshore financial sector with 84 trust service companies providing financial and administrative services to an international clientele, which includes offshore companies, mutual funds, and international finance companies. As of September 2007, there were a total of 14,191 offshore companies registered with the Chamber of Commerce in the Netherlands Antilles, as is required by law. International corporations may be registered using bearer shares. The practice of the financial sector in the Netherlands Antilles is for either the bank or the company service providers to maintain copies of bearer share certificates for international corporations, which include information on the beneficial owner(s). The Netherlands Antilles also permits Internet gaming companies to be licensed on the islands. There are currently four-operator member and nine-nonoperator member licensed Internet gaming companies.

In February 2001, the GONA approved proposed amendments to the free zone law to allow e-commerce activities into these areas (National Ordinance Economic Zone no.18, 2001). It is no longer necessary for goods to be physically present within the zone as was required under the former free zone law. Furthermore, the name "Free Zone" was changed to "Economic Zone" (e-zone). Seven areas within the Netherlands Antilles qualify as e-zones, five of which are designated for e-commerce. The remaining two e-zones, located at the Curacao airport and harbor, are designated for goods. These zones are minimally regulated; however, administrators and businesses in the zones have indicated an interest in receiving guidance on detecting unusual transactions.

Money laundering is a criminal offense in the Netherlands Antilles under the 1993 National Ordinance on the penalization of money laundering (O.G. 1993, no. 52), as amended by a 2001 National Ordinance (O.G. 2001, no. 77). This legislation establishes that prosecutors do not need to prove that a suspected money launderer also committed an underlying crime to obtain a money laundering conviction. In recent years, the GONA has taken steps to strengthen its anti-money laundering regime

by expanding suspicious activity reporting requirements to nonfinancial sectors; introducing indicators for the reporting of unusual transactions for the gaming industry; issuing guidelines to the banking sector on detecting and deterring money laundering; and modifying existing money laundering legislation that penalizes currency and securities transactions by including the use of valuable goods. A GONA interagency anti-money laundering working group cooperates with its Kingdom counterparts.

Both bank and nonbank financial institutions, such as company service providers and insurance companies, are required by law to report suspicious transactions to the financial intelligence unit (FIU), the Meldpunt Ongebruikelijke Transacties (MOT NA). Obligated entities are also required to report all transactions over NAF 250,000 (approximately U.S. $142,000). Banks are required to maintain records for ten years and all other financial intermediaries must maintain records for five years. The GONA is currently amending its legislation to add designated nonfinancial businesses and professions as reporting entities, including lawyers, accountants, notaries, jewelers and real estate agents. It is expected that the legislation will be passed in 2008. Obligated entities are required to report suspected terrorist financing activity to the MOT NA as well, although terrorist financing is not a criminal offense in the Netherlands Antilles.

The MOT NA was established under the Ministry of Finance in 1997. Through October 2006, the MOT NA received 10,788 suspicious transaction reports totaling U.S. $1.3 billion. Of these, 283 were reported to the relevant law enforcement authorities. No statistics are currently available for 2007. The MOT NA currently has a staff of nine, and is engaged in increasing the effectiveness and efficiency of its reporting system. Progress has been reported in automating suspicious activity reporting. Additionally, the MOT NA has issued a manual for casinos on how to file reports and has started to install software in casinos that will allow reports to be submitted electronically. The MOT NA hosted a Kingdom of the Netherlands seminar in October 2007. The Government of the Netherlands plans to provide technical support to the MOT NA to improve their analytical capabilities with regard to terrorist financing.

The Central Bank of the Netherlands Antilles supervises all banking and credit institutions, including banks for local and international business, specialized credit institutions, savings banks, credit unions, credit funds, and pension funds. The Central Bank also supervises insurance companies, insurance brokers, mutual funds and administrators of these funds, and company service providers, all of which must be licensed by the Central Bank. The Central Bank has issued anti-money laundering guidelines for banks, insurance companies, pension funds, money transfer services, financial administrators, and company service providers. The guidelines also specifically include terrorist financing indicators. Entities under supervision must submit an annual statement of compliance. The Central Bank has provided training to different sectors on the guidelines. The Central Bank also established the Financial Integrity Unit to monitor corporate governance and market behavior.

As of May 2002, all persons entering or leaving one of the island territories of the Netherlands Antilles must report of the transportation of NAF 20,000 (approximately U.S. $11,300) or more in cash or bearer instruments to Customs officials. This provision also applies to those entering or leaving who are demonstrably traveling together and who jointly carry with them money for a value of NAF 20,000 or more. Declaration of currency exceeding the threshold must include origin and destination. Violators may be fined up to NAF 250,000 (approximately U.S. $142,000) and/or face one year in prison.

In 2000, the GONA enacted the National Ordinance on Freezing, Seizing and Forfeiture of Assets Derived from Crime. The law allows the prosecutor to seize the proceeds of any crime proven in court. Civil forfeiture is not permitted.

Terrorist financing is not a separate crime in the Netherlands Antilles, although acts that can be considered to support terrorism are criminalized in Articles 49 and 50 of the Criminal Code. Although

terrorist financing is not per se a crime, the GONA enacted legislation in 2002 allowing a judge or prosecutor to freeze assets related to the Taliban and Usama Bin Laden, as well as all persons and companies connected with them. The legislation contains a list of individuals and organizations suspected of terrorism. The Central Bank instructed financial institutions to query their databases for information on the suspects and to immediately freeze any assets found. In October 2002, the Central Bank instructed the financial institutions under its supervision to continue these efforts and to consult the UN website for updates to the list.

Netherlands Antilles' law allows the exchange of information between the MOT NA and foreign FIUs by means of memoranda of understanding and by treaty. The MOT NA's policy is to answer requests within 48 hours of receipt. A tax information exchange agreement (TIEA) between the Netherlands and the United States with regard to the Netherlands Antilles, signed in 2002, entered into force in March 2007. The Mutual Legal Assistance Treaty between the Netherlands and the United States applies to the Netherlands Antilles; however, the treaty is not applicable to requests for assistance relating to fiscal offenses addressed to the Netherlands Antilles. The U.S.-Netherlands Agreement Regarding Mutual Cooperation in the Tracing, Freezing, Seizure and Forfeiture of Proceeds and Instrumentalities of Crime and the Sharing of Forfeited Assets also applies to the Netherlands Antilles.

The MOT NA is a member of the Egmont Group. The Netherlands Antilles is a member of the Caribbean Financial Action Task Force (CFATF), and as part of the Kingdom of the Netherlands, participates in the Financial Action Task Force (FATF). The Netherlands Antilles is also a member of the Offshore Group of Banking Supervisors. The Kingdom of the Netherlands has extended its ratification of the 1988 UN Drug Convention to the Netherlands Antilles. The Kingdom of the Netherlands became a party to the UN International Convention for the Suppression of the Financing of Terrorism in 2002. In accordance with Netherlands Antilles' law, which stipulates that all the legislation must be in place prior to ratification, the GONA is preparing legislation to enable the Netherlands to extend ratification of the Convention to the Netherlands Antilles. Likewise, the Kingdom of the Netherlands has not yet extended ratification of the UN Convention against Transnational Organized Crime or the UN Convention against Corruption to the Netherlands Antilles.

The Government of the Netherlands Antilles has demonstrated a commitment to combating money laundering. However, the GONA should criminalize the financing of terrorism and enact the necessary legislation to implement the UN International Convention for the Suppression of the Financing of Terrorism. The Netherlands Antilles should also continue its focus on increasing regulation and supervision of the offshore sector and free trade zones, as well as pursuing money laundering investigations and prosecutions. The GONA should ensure that anti-money laundering regulations and reporting requirements are extended to designated nonfinancial businesses and professions.

## Nicaragua

Nicaragua is not a regional financial center or a major drug producing country. However, it continues to serve as a significant transshipment point for South American cocaine and heroin destined for the United States and—on a smaller scale—for Europe. There is evidence that the narcotics trade is increasingly linked to arms trafficking. This situation, combined with weak adherence to the rule of law, judicial corruption, the politicization of the public prosecutor's office and the Supreme Court, and insufficient funding for law enforcement institutions, makes Nicaragua's financial system an attractive target for money laundering. Nicaragua's geographical position—with access to both the Atlantic and the Pacific Oceans, porous border crossings to its north and south, and a lightly inhabited and underdeveloped Atlantic Coast area—makes it an area heavily used by transnational organized crime groups. These groups also benefit from Nicaragua's weak legal system and its ineffective fight against financial crimes, money laundering, human trafficking, and the financing of terrorism. Nicaraguan officials have expressed concern that, as neighboring countries have tightened their anti-money

laundering laws, established financial intelligence units (FIUs), and taken other enforcement actions, more illicit money has moved into the vulnerable Nicaraguan financial system.

Nicaragua does not permit direct offshore bank operations, but it does permit such operations through nationally chartered entities. Bank and company bearer shares are permitted. Nicaragua has a well-developed indigenous gaming industry, which remains largely unregulated. Two competing casino regulation bills are currently in the National Assembly; the main difference between the bills is whether regulatory authority will fall under the tax authority or if an independent institution will be established to supervise the industry. There are no known offshore or Internet gaming sites in Nicaragua.

A number of foreign institutions own significant shares of the Nicaraguan financial sector. In 2008, GE Consumer Finance, one of the largest financial service firms in the world, will become the owner of Banco de America Central (BAC), which operates in several Central American countries, including Nicaragua. In 2007, HSBC purchased Banistmo, a Panamanian bank, and now operates under that name in Nicaragua. Most large Nicaraguan banks already maintain correspondent relationships with Panamanian institutions.

The entry into force of the Central America/Dominican Republic Free Trade Agreement (CAFTA-DR) in 2006 and the increased pace of regional integration suggest growing involvement of Nicaraguan financial institutions with international partners and clients. A new free trade agreement (FTA) with Taiwan will go into effect in 2008, which should expand Nicaragua's financial relationships with Asia. Nicaragua also just concluded FTA negotiations with Panama and, along with its Central American neighbors, is expected to begin negotiating an FTA with the EU.

As of January 2007, a total of 109 companies operate in 38 designated free trade zones (FTZs) in Nicaragua. As of December 2006, an estimated 80,000 persons were employed by companies operating in FTZs, producing a total of $900 million in export sales. The National Free Trade Zone Commission (CNZF), a state-owned corporation, regulates all FTZs and the companies located in them. The Nicaraguan Customs Agency also monitors all imports and exports of FTZ companies. While there is no indication that these FTZs are being used in trade-based money laundering schemes or by the financiers of terrorism, a June 2007 inspection by U.S. Customs agents uncovered evidence of transshipments of Chinese-made apparel.

On November 13, 2007, Nicaragua's National Assembly passed a new penal code that criminalizes terrorist financing, bulk cash smuggling, and money laundering beyond drug-related offenses. The penal code also expands legal protection for the financial sector, and defines crimes against the banking and financial system. When implemented, the new penal code should bring Nicaragua's anti-money laundering and counter-terrorist financing regime into greater compliance with the international standards of the Financial Action Task Force. However, the penalty for committing money laundering is still relatively low by international standards, with a sentence of five to seven years. The new penal code does not provide for the creation of an FIU.

While the adoption of the new penal code demonstrates the Government of Nicaragua's (GON) commitment to fight the financing of terrorism, money laundering, and other financial crimes, limited resources, corruption (including in the judiciary), and the lack of political will in some sectors continue to complicate efforts to counteract these criminal activities. Nicaragua has recently made improvements to its oversight and regulatory control of its financial system. Although the current Prosecutor General once advocated a narrow interpretation of money laundering law that only would penalize the laundering of proceeds from narcotics trafficking and not from other illegal activities, he now supports the formation of an FIU and by extension the prosecution of a wider range of money laundering-related offenses. However, the National Prosecutor's Office has still failed to prosecute a single money laundering case. This enforcement problem is exacerbated by the fact that the country

does not have an operational FIU. The National Prosecutor's Office has prosecuted at least four cases of cash smuggling, although these crimes are currently considered only customs violations.

Law 285 of 1999 requires all financial institutions (including stock exchanges and insurance companies) under the supervision of the Superintendence of Banks and Other Financial Institutions (SIBOIF) to report cash deposits over $10,000 and suspicious transactions to the SIBOIF and to keep records for five years. The SIBIOF then forwards the reports to the Commission of Financial Analysis (CAF). All persons entering or leaving Nicaragua are also required to declare the transportation of currency in excess of U.S. $10,000 or its equivalent in foreign currency. All financial institutions not supervised by SIBIOF are required to report suspicious transactions directly to the CAF. Bank officials are held responsible for all of their institution's actions, including failure to report money laundering, and sanctions may be imposed on financial institutions and professionals of the financial sector, including internal auditors, who do not develop anti-money laundering programs or do not report to the appropriate authorities suspicious and unusual transactions that may be linked to money laundering, as required by the anti-money laundering law.

The SIBOIF is considered to be an independent and reputable financial institution regulator. The position of the Superintendent does not enjoy legal immunity, exposing the Superintendent to lawsuits from regulated institutions. Officers in financial institutions charged with reporting suspicious transactions to the SIBOIF are also unprotected legally with regard to their cooperation. Given the corruption in the judicial system, this exposure can limit the willingness of SIBIOF to make "unpopular" decisions; however, the institution's financial experts have reached out to the Nicaraguan National Police (NNP) to work with them. The SIBIOF has regularly fined banks for not reporting suspicious transactions. The willingness of the SIBIOF and NNP to investigate financial crimes, and a substantial level of cooperation between the Attorney General's Office and the NNP on financial crimes and money laundering issues, has resulted in a greater adherence by banks to the reporting requirements contained in Law 285.

On paper, the CAF is comprised of representatives from various elements of law enforcement and banking regulators and is responsible for detecting money laundering trends, coordinating with other agencies and reporting its findings to Nicaragua's National Anti-Drug Council. The CAF does not analyze the information received, and is not considered to be a professional or independent unit. It is ineffective due to an insufficient budget, the politicization of its leadership, and a lack of fully dedicated, trained personnel, equipment and strategic goals. All of its members have primary responsibilities in their parent institutions, which take precedence over CAF duties. The CAF is headed by the National Prosecutor, who receives the reports from banks and decides whether to refer them to the NNP for further investigation.

The NNP's Economics Crimes Unit and the Office of the National Prosecutor are in charge of investigating financial crimes, including money laundering and terrorist financing. The Office of the National Prosecutor is in the process of creating its Economic Crimes Unit to work in tandem with the NNP. The United States has successfully supported the creation of a vetted unit within the NNP. The unit has been conducting investigations into money laundering and drug related crimes since March 2007 and is expected to work closely with the Attorney General's office.

In October 2007, following publicity that highlighted the consequences of Nicaragua's being one of the few countries in Latin America without an FIU, the National Assembly renewed debate on a 2004 bill creating an independent FIU. The 2004 bill creates a central, independent FIU that would replace and enhance the functions of the CAF and establish more stringent reporting requirements. In August 2007, the SIBIOF suggested amendments to the bill before the National Assembly that would bring the proposed FIU into compliance with all Egmont Group of FIUs requirements.

Under the new penal code adopted by the National Assembly in November 2007, terrorism and its financing are now crimes in Nicaragua. Through five SIBIOF administrative decrees, the GON also

has the authority to identify, freeze, and seize terrorist-related assets, but has not as yet identified any such active cases. Reportedly, there are no hawala or other similar alternative remittance systems operating in Nicaragua, and the GON has not detected any use of gold, precious metals or charitable organizations to disguise transactions related to terrorist financing. However, there are informal "cash and carry" networks for delivering remittances from abroad.

There are over 300 micro-finance institutions (MFI) in Nicaragua, serving over 300,000 clients and handling over U.S. $400 million. MFIs in Nicaragua dominate the informal economy and manage a significant portion of the remittances. Over half of this market is handled by five institutions that have now converted to become formal banks. One institution, Banco Pro-Credit, is a branch of a German MFI institution that also has branches in Eastern Europe and Africa. The MFI sector has grown steadily at about 25 percent per year since 1999. While the five MFIs that are now formal banks are regulated by the SIBIOF, all the others are currently unregulated. These institutions are, however, still subject to the reporting requirements in Law 285 and to financial crimes listed in the current Penal Code. Any crimes committed fall under the jurisdiction of the Economic Crimes unit of the National Police and the National Prosecutor's Office.

Nicaragua is a party to the 1988 United Nations Drug Convention, the UN International Convention on the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. The GON has also ratified the Inter-American Convention on Mutual Legal Assistance in Criminal Matters and the Inter-American Convention against Terrorism. Nicaragua is a member of the Money Laundering Experts Working Group of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD), and the Caribbean Financial Action Task Force (CFATF). Due to Nicaragua's failure to establish a functional FIU, it is the only country in Central America and one of the only countries in the Americas that does not have an FIU and is not a member of the Egmont Group of FIUs. Due to corruption in the Nicaraguan judiciary, the United States has cut off direct assistance to the Nicaraguan Supreme Court.

The Government of Nicaragua has made progress in its efforts to combat financial crime by expanding the predicate crimes for money laundering beyond narcotics trafficking and criminalizing terrorist financing. However, the GON also needs to allocate the necessary resources to develop an effective financial intelligence unit, and combat corruption. Nicaragua should develop a more effective method of obtaining information and cooperation from foreign law enforcement agencies and banks, take steps to immobilize its bearer shares and adequately regulate its gambling industry. These actions, coupled with increased enforcement, would significantly strengthen the country's financial system against money laundering and terrorist financing, and would bring Nicaragua closer to compliance with relevant international anti-money laundering and counter-terrorist financing standards and controls.

## Nigeria

Although the Federal Republic of Nigeria is not an offshore financial center, Nigeria's large economy is a hub for the trafficking of persons and narcotics. Nigeria is a major drug-transit country and is a center of criminal financial activity, reportedly for the entire continent. Individuals and criminal organizations have taken advantage of the country's location, weak laws, systemic corruption, lack of enforcement, and poor socioeconomic conditions to strengthen their ability to perpetrate financial crimes at home and abroad. Nigerian criminal organizations are adept at devising new ways of subverting international and domestic law enforcement efforts and evading detection. Their success in avoiding detection and prosecution has led to an increase in many types of financial crimes, including bank fraud, real estate fraud, and identity theft. In addition, advance fee fraud, also referred to internationally as "419" fraud, in reference to the fraud section in Nigeria's criminal code, is a lucrative financial crime that generates hundreds of millions of illicit dollars annually for criminals.

Despite years of government effort to counter rampant crime and corruption, Nigeria continues to be plagued by crime. The establishment of the Economic and Financial Crimes Commission (EFCC) along with the Independent Corrupt Practices Commission (ICPC) and the improvements in training qualified prosecutors for Nigerian courts yielded some successes in 2006 and 2007.

In June 2001, the Financial Action Task Force (FATF) placed Nigeria on its list of noncooperative countries and territories (NCCT). In December 2002, Nigeria enacted two pieces of legislation to remedy the deficiencies. It passed an amendment to the 1995 Money Laundering Act extending the scope of the law to cover the proceeds of all crimes. The Government of Nigeria (GON) also passed an amendment to the 1991 Banking and Other Financial Institutions (BOFI) Act expanding coverage of the law to stock brokerage firms and foreign currency exchange facilities, giving the Central Bank of Nigeria (CBN) greater power to deny bank licenses, and allowing the CBN to freeze suspicious accounts. The third piece of legislation, the 2004 Economic and Financial Crimes Commission (Establishment) Act, established the Economic and Financial Crimes Commission (EFCC), the body that investigates and prosecutes money laundering and other financial crimes, and coordinates information sharing. The Economic and Financial Crimes Commission Act also criminalizes the financing of terrorism and participation in terrorism. Violation of the Act carries a penalty of up to life imprisonment. In May 2006, the FATF visited Nigeria to conduct an evaluation of the revisions made to the government's AML regime. FATF recognized that the GON had remedied the major deficiencies in its anti-money laundering (AML) regime and removed Nigeria from the NCCT list.

Since its inception in April 2004, the EFCC has had the mandate to investigate and prosecute financial crime. It has recovered or seized assets from people guilty of fraud both inside and outside of Nigeria, including a syndicate that included highly placed government officials who were defrauding the Federal Inland Revenue Service (FIRS). Several influential individuals have been arrested and are currently awaiting trial. EFCC members also embarked upon a campaign to identify and prosecute former officials. Some EFCC members have been killed for their efforts to expose and enforce the laws against corruption and financial crime.

The National Assembly passed the Money Laundering (Prohibition) Act (2004), which applies to the proceeds of all financial crimes. Nigeria also employs the 1995 Foreign Exchange (Monetary and Miscellaneous Provisions) Act. The legislation gives the CBN greater power to deny bank licenses and freeze suspicious accounts. This legislation also strengthens financial institutions by requiring more stringent identification of accounts, removing a threshold for suspicious transactions, and lengthening the period for retention of records. Money laundering controls apply to banks and other financial institutions, including stock brokerages and currency exchange house, as well as designated nonfinancial businesses and professions (DNFBPs). These institutions include dealers in jewelry, cars and luxury goods, chartered accountants, audit firms, tax consultants, clearing and settlement companies, legal practitioners, hotels, casinos, supermarkets and other businesses that the Federal Ministry of Commerce designates as obliged. The EFCC Act provides safe-harbor provisions to obliged entities. Nigeria has no secrecy laws that prevent the disclosure of client and ownership information by domestic financial services companies to bank regulatory and law enforcement authorities.

The Special Control Unit Against Money Laundering (SCUML), is a special unit in the Ministry of Commerce which monitors, supervises, and regulates the activities of all DNFBPs. Oversight, however, has reportedly not been very rigorous or effective. Amendments to the 2004 EFCC Act gave the EFCC the authority to investigate and prosecute money laundering, enlarged the number of EFCC board members, enabled the EFCC police members to bear arms, and banned interim court appeals that hinder the trial court process.

The Nigerian Financial Intelligence Unit (NFIU), established in 2005, derives its powers from the Money Laundering (Prohibition) Act of 2004 and the Economic and Financial Crimes Commission

Act of 2004. Housed within the EFCC, it is the central agency for the collection, analysis and dissemination of information on money laundering and terrorist financing. The NFIU is a significant component of the EFCC, complementing the EFCC's directorate of investigations. It does not carry out its own investigations. Legal provisions give the NFIU power to receive suspicious transaction reports (STRs) submitted by financial institutions and designated nonfinancial businesses and professions. The NFIU also receives reports involving the transfer to or from a foreign country of funds or securities exceeding U.S. $10,000 in value. All financial institutions and designated nonfinancial institutions are required by law to furnish the NFIU with details of these financial transactions.

The NFIU fulfills a crucial role in receiving and analyzing STRs. As a result of the NFIU's activities, banks have improved both their timeliness and quality in filing STRs reported to the NFIU. The NFIU has access to records and databanks of all government and financial institutions, and it has entered into memoranda of understandings (MOUs) on information sharing with several other FIUs. In 2006, the NFIU received 3,772,843 currency transaction reports (CTRs). Out of the 47 cases the NFIU developed, 12 investigations are ongoing, and the NFIU disseminated 18 and placed 10 under monitoring. The NFIU closed seven in-house cases. Because the disseminated cases are still under investigation, no formal feedback came from stakeholders in either 2006 or 2007. There were 73 money laundering convictions from January 2005 through October 2006. The trial court process has improved after several experienced judges received assignations specifically to handle EFCC cases; encouraged, EFCC officials have brought more cases to court. Additional information for 2007 is not available.

Due to the EFCC's activities, the enactment of new laws, and a public enlightenment campaign, crimes such as bank fraud and counterfeiting have been reported and prosecuted, sometimes for the first time. The EFCC is the agency with the most capacity to effectively investigate and prosecute financial crimes, including money laundering and terrorist financing. The EFCC coordinates agencies' efforts in pursuing financial crime investigations. In addition to the EFCC, the National Drug Law Enforcement Agency (NDLEA), the Independent Corrupt Practices Commission (ICPC), and the Criminal Investigation Department of the Nigeria Police Force (NPF/CID) are empowered to investigate financial crimes. Reportedly, the Nigerian Police Force is incapable of handling financial crimes because of alleged corruption and poor institutional capacity.

In 2007, the EFCC marked significant successes in combating financial crime. Through EFCC efforts, a former inspector general of police was arrested and prosecuted for financial crimes valued at over U.S. $13 million. The GON seized his assets and froze his bank accounts. Currently serving a prison sentence, he still faces 92 charges of money laundering and official corruption. Five former state governors are under investigation for money laundering. The EFCC is working with the FBI on a case involving a group of money brokers laundering money through banks in the United States. In 2006, the EFCC received a surge of petitions and leads provided by whistleblowers. Reportedly, many of these alleged abuses of office involved politically exposed persons (PEPs) and/or their collaborators. As the period coincided with preparations for the general elections in 2007, some of the investigations were politically charged. The Legal and Prosecution Unit, responsible for the prosecution of all cases, is examining 437 of these cases for possible prosecution.

The Unit prosecuted several high profile cases involving powerful and well connected persons and their associates. The EFCC filed 588 cases between 2006 and mid-2007. In 2007, the Legal Unit had obtained 53 convictions by mid-year. Investigations led to the recovery of approximately 30 billion naira (approximately U.S. $259 million). Suspects returned several other billions of naira when it became apparent that the Commission was about to expose the abuses. Some governors were arrested for laundering their state government funds. The Executive Chairman, appearing before the Senate to present a report of the Commission's activities, revealed allegations of corrupt practices and abuse of office reportedly associated with 31 out of the 36 then serving Governors. Some of the Governors had

constitutional immunity that expired in May 2007. They are now standing trial in various courts for various offenses including money laundering.

While the NDLEA has the authority to handle narcotics-related cases, it does not have adequate resources to trace, seize, and freeze assets. Cases of this nature are usually referred to the EFCC. Depending on the nature of the case, the tracing, seizing, and freezing of assets may be executed by the EFCC, NDLEA, NPF, or the ICPC. The proceeds from seizures and forfeitures pass to the federal government, and the GON uses a portion of the recovered sums to provide restitution to the victims of the criminal acts. The banking community is cooperating with law enforcement to trace funds and seize or freeze bank accounts. Since its establishment the EFCC has reportedly seized assets worth $5 billion.

Section 20 of the 2004 EFCC Act provides for the forfeiture of assets and properties to the federal government after a money laundering conviction. Foreign assets are also subject to forfeiture. The properties subject to forfeiture are set forth in EFCC Act Sections 24-26, and include any real or personal property representing the gross receipts a person obtains directly as a result of the violation of the act, or traceable to such receipts. They also include any property representing the proceeds of an offense under the laws of a foreign country within which the offense or activity would be punishable for more than one year. All means of conveyance, including aircraft, vehicles, or vessels used or intended to be used to transport or facilitate the transportation, sale, receipt, possession or concealment of the economic or financial crimes is likewise subject to forfeiture. Forfeiture is possible only as part of a criminal prosecution. There is no comparable law providing for civil forfeiture independent of a criminal prosecution, but the EFCC has established a committee addressing this deficiency by drafting legislation.

The EFCC has the authority to prevent the use of charitable and nonprofit entities as money laundering vehicles, although it has not reported any cases involving these entities.

Nigerian criminals initially made the advance fee fraud scheme infamous. Today, nationals of many African countries and from a variety of countries around the world also perpetrate advance fee fraud. While there are many variations, the main goal of 419 frauds is to deceive victims into the payment of a fee by persuading them that they will receive a very large benefit in return, or by persuading them to pay fees to “rescue” or help a newly-made “friend” in some sort of alleged distress. A majority of these schemes end after the victims have suffered monetary losses, but some have also involved kidnapping, and/or murder. Perpetrators use the Internet to target businesses and individuals around the world.

The Government of Nigeria continued throughout 2007 with its efforts to eradicate 419 crimes. GON efforts previously led to the successful prosecution and conviction of a number of them, but the problem is far from over. Following the promulgation of the Advance Fee Fraud Act 2006 the EFCC held an interactive session with stakeholders. The EFCC also briefed cyber cafe operators, business centers, Internet service providers, telecommunication companies and banks on their responsibilities under the new law. One of their requirements is to register their businesses with the EFCC. To keep pace with the sophistication with which the fraudsters operate, the EFCC deployed interception technology to enhance the investigation of crimes, particularly those committed through cyberspace. The Advance Fee Fraud Unit burst several employment, credit card, and e-payment scams, shut down several domains and cloned websites, raided residential houses, seized computers, and blocked fraudulent e-mail addresses, telephone lines and faxes associated with cybercrimes. Despite the progress the EFCC has made, there have been few recorded successes as a result of the EFCC’s cybercrime initiatives.

The EFCC’s success in investigating and prosecuting financial crime, especially high-level corruption, has brought it both the support of the international community and the ire of corrupt officials. In December 2007, the Government of Nigeria reassigned the EFCC Chairman, the country’s highest

ranking and most publicly visible anti-corruption official, Nuhu Ribadu, to a year-long training course. This reassignment coincides with the high-profile trials of several officials, including seven former governors. Ribadu has served as the face of Nigerian AML/CTF efforts, and his removal could undermine the perception of the GON's commitment to fighting corruption. The reassignment of Ribadu may also impact the NFIU's autonomy and its ability to act independently.

Nigeria criminalized the financing of terrorism under the Economic and Financial Crimes Commission (Establishment) Act of 2004. The EFCC has authority under the act to identify, freeze, seize, and forfeit terrorist finance-related assets. Nigerian financial institutions periodically receive the UNSCR 1267 Sanctions Committee's consolidated list, but have not yet detected a case of terrorist financing within the banking system.

Nigeria 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, and the UN Convention against Corruption. Nigeria has also ratified the African Union Convention on the Prevention and Combating of Terrorism and the African Union Convention on Preventing and Combating Corruption. Nigeria ranks 147 out of 180 countries in Transparency International's 2007 Corruption Perceptions Index.

The United States and Nigeria have a Mutual Legal Assistance Treaty, which entered into force in January 2003. Nigeria has signed memoranda of understanding with Russia, Iran, India, Pakistan and Uganda to facilitate cooperation in the fight against narcotics trafficking and money laundering. Nigeria has also signed bilateral agreements for exchange of information on money laundering with South Africa, the United Kingdom, and all Commonwealth and Economic Community of West African States countries. The EFCC worked with foreign partners to raid notorious cyber cafes to curtail the activities of the 419 fraudsters. The EFCC collaborated with the United States Postal Service and the UK Serious and Organized Crime Agency (SOCA) to intercept over 15,000 counterfeit checks. A collaboration scheme between the EFCC, the United States, the UK and the Dutch was constituted to more effectively address the problem of international fraud, including identity theft and e-marketing fraud. Nigeria is a member of the Intergovernmental Task Force against Money Laundering in West Africa (GIABA), a FATF-style regional body. During 2007, Nigeria held the Directorship General of GIABA. The NFIU is a member of the Egmont Group.

The Government of Nigeria continued to pursue money laundering both within and outside the country in 2007. Nigeria should continue to pursue its anti-corruption program and support both the ICPC and EFCC in their mandates to investigate and prosecute corrupt government officials and individuals. Nigeria should take steps to ensure the autonomy and independence of those entities. GON should strengthen the authority of the SCUML to supervise designated nonfinancial businesses and professions by moving the Special Control Unit out from under the Ministry of Commerce. The GON should continue to engage with the FATF and other relevant international organizations to identify and eliminate remaining anti-money laundering deficiencies. Nigeria should ensure that the Police Force has the capacity to function as an investigative partner in financial crime cases, as well as work to eradicate any corruption that might exist within that and other law enforcement bodies. Nigeria should continue to support the EFCC's efforts, including drafting a law for civil forfeiture provisions to the AML/CTF framework, and pursuing those who commit financial crime, regardless of political status. Nigeria should continue towards implementation of a comprehensive AML regime that promotes respect the rule of law; willingly shares information with foreign regulatory and law enforcement agencies; is capable of thwarting money laundering and terrorist financing; and maintains compliance with all relevant international standards.