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

Iraq

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

The Coalition Provisional Authority (CPA), the international body that governed Iraq beginning in April 2003, issued regulations and orders that carried the weight of law in Iraq. The CPA ceased to exist in June 2004, at which time the Iraqi Interim Government assumed authority for governing Iraq. Drafted and agreed to by Iraqi leaders, the Transitional Administrative Law (TAL) described the powers of the Iraqi government during the transition period. Under TAL Article 26, regulations and orders issued by the CPA pursuant to its authority under international law remain in force until rescinded or amended by legislation duly enacted and having the force of law. The constitution, which was ratified in October 2005, also provides for the continuation of existing laws, including CPA regulations and orders that govern money laundering.

The CPA Order No. 93, "Anti-Money Laundering Act of 2004" (AMLA) governs financial institutions in connection with: money laundering, financing of crime, financing terrorism, and the vigilance required of financial institutions in regard to financial transactions. The law also criminalizes money laundering, financing crime (including the financing of terrorism), and structuring transactions to avoid legal requirements. The AMLA covers: banks; investment funds; securities dealers; insurance entities; money transmitters and foreign currency exchange dealers, as well as persons who deal in financial instruments, precious metals or gems; and persons who undertake hawala transactions. Covered entities are required to verify the identity of any customer opening an account for any amount. Covered entities are also required to verify the identity of non-account holders performing a transaction or series of potentially related transactions whose value is equal to or greater than five

million Iraqi dinars (approximately $3,500). Beneficial owners must be identified upon account opening or for transactions exceeding ten million Iraqi dinar (approximately $7,000). Records must be maintained for at least five years. Covered entities must report suspicious transactions and wait for guidance before proceeding with the transaction; the relevant funds are frozen until guidance is received. Suspicious transaction reports (STRs) are to be completed for any transaction over four million Iraqi dinar (approximately $3,000) that is believed to involve funds that are derived from illegal activities or money laundering, intended for the financing of crime, (including terrorism), or over which a criminal organization has disposal power, or a transaction conducted to evade any law and which has no apparent business or other lawful purpose. The "tipping off" of customers by bank employees where a transaction has generated a suspicious transaction report is prohibited. Bank employees are protected from liability for cooperating with the government. Willful violations of the reporting requirement may result in imprisonment or fines.

CPA Order No. 94, "Banking Law of 2004," gives the Central Bank of Iraq (CBI) the authority to license banks and to conduct due diligence on proposed bank management. Order No. 94 establishes requirements for bank capital, confidentiality of records, audit and reporting requirements for banks, and prudential standards. The CBI is responsible for the supervision of financial institutions. The CBI was mandated by the AMLA to issue regulations and require financial institutions to provide employee training, appoint compliance officers, develop internal procedures and controls to deter money laundering, and establish an independent audit function. The AMLA provides that the CBI will issue guidelines on suspicious financial activities and conduct on-site examinations to determine institutions' compliance. The CBI also may issue regulations to require large currency transaction reports for the cross-border transport of currency of more than 15 million Iraqi dinars (approximately $10,000). Neither Iraqis nor foreigners are permitted to transport more than $10,000 in currency when exiting Iraq. The CBI is also mandated by the AMLA to distribute the UN 1267 Sanction Committee's consolidated list of suspected terrorists or terrorist organizations. No asset freezes pertaining to any names on the consolidated list have been reported to date. Order No. 94 gives administrative enforcement authority to the CBI, up to and including the removal of institution management and revocation of bank licenses.

The AMLA calls for the establishment of the Money Laundering Reporting Office (MLRO) within the CBI. The MLRO was recently formed in June/July 2006 and has a small but dedicated staff. The CBI and representatives from the United States are working together to build the MLRO's capacity and implement the day-to-day functions of a financial intelligence unit (FIU). The MLRO will operate independently to collect, analyze and disseminate information on financial transactions subject to financial monitoring and reporting, including suspicious activity reports. The MLRO is also empowered to exchange information with other Iraqi or foreign government agencies. The CBI and its MLRO finalized implementing regulations to the AMLA, which became effective September 15, 2006.

The predicate offenses for the crimes of money laundering and the financing of crime are quite broad and extend beyond "all serious offenses" to include "some form of unlawful activity." The penalties for violating the AMLA depend on the specific nature of the underlying criminal activity. For example, "money laundering" is punishable by a fine of up to 40 million dinar (approximately $27,080), or twice the value of the property involved in the transaction (whichever is greater), or imprisonment of up to four years, or both. Other offenses for which there are specific penalties include the financing of crime (a fine of up to 20 million dinar (approximately $13,540), two years' imprisonment, or both) and structuring transactions (up to 10 million dinar (approximately $6,770), one year imprisonment, or both). No arrests or prosecutions under the AMLA have been reported to date.

The AMLA includes provisions for the forfeiture of any property Such property includes, but is not limited to, funds involved in a covered offense, or any property traceable to the property, or any

property gained as a result of such an offense, without prejudicing the rights of bona fide third parties. The AMLA also blocks any funds or assets, other than real property (which is covered by a separate regulation), belonging to members of the former Iraqi regime and authorizes the Minister of Finance to confiscate such assets following a judicial or administrative order. The lack of automation or infrastructure in the banking sector, however, hinders the government's ability to identify and freeze assets linked to illicit activity.

Iraq has free trade zones in Basra/Khor al-Zubair, Ninewa/Falafel, Sulaymaniyah, and Al-Quaymen. Under the Free Zone (FZ) Authority Law, goods imported and exported from the FZ are generally exempt from all taxes and duties, unless the goods are imported into Iraq. Additionally, capital, profits, and investment income from projects in the FZ are exempt from taxes and fees throughout the life of the project, including in the foundation and construction phases.

Iraq became a member of the Middle East and North Africa Financial Action Task Force (MENAFATF) in September 2005. Iraq is a party to the 1988 UN Drug Convention, but not the UN International Convention for the Suppression of the Financing of Terrorism or the UN Convention against Transnational Organized Crime.

In 2006, in a challenging environment, the Government of Iraq continued to lay the foundation for anti-money laundering and counterterrorist finance regimes. In these efforts, there was strong cooperation with the U.S. Government. However, there is much work ahead. Iraq should become a party to the UN Conventions for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. It should take a more active part in MENAFATF and implement its recommendations. Iraq should continue its efforts to build capacity and actively implement the provisions of the AMLA and related authorities. As a priority, as Iraq's MLRO becomes fully functional, it should develop increased capacity to investigate financial crimes and enforce the provisions of the AMLA. Iraqi law enforcement, border authorities, and customs service should strengthen border enforcement and identify and pursue smuggling and trade-based money laundering networks. Increased border enforcement is also a prerequisite in combating terrorist finance. Iraq should also take concerted steps to combat corruption.

Ireland

Ireland is an increasingly significant European financial hub, with the international banking and financial services sector concentrated in Dublin's International Financial Services Centre (IFSC). Narcotics trafficking, fraud, and tax offenses are the primary sources of funds laundered in Ireland. Money laundering occurs in credit institutions, although launderers have also made use of money remittance companies, solicitors, accountants, and second-hand car dealerships. The most common laundering methods are: the purchase of high-value goods for cash; the use of credit institutions to receive and transfer funds in and out of Ireland; the use of complex company structures to filter funds; and the purchase of properties in Ireland and abroad.

The Shannon Free Zone was established in 1960 as a free trade zone, offering investment incentives for multinational companies. The Shannon Free Zone is supervised by "Shannon Development," a government-founded body. Reportedly, there are no indications that the Shannon Free Zone is being used in trade-based money laundering schemes or by financiers of terrorism.

The international banking and financial services sector concentrated in Dublin's International Financial Services Centre (IFSC). In 2006, there were approximately 430 international financial institutions and companies operating in the IFSC. Services offered include banking, fiscal management, re-insurance, fund administration, and foreign exchange dealing. The use of offshore bank accounts, the creation of shell corporations and trusts, all of which obfuscate the true beneficial owner are additional sources of money laundering that represent significant vulnerabilities common to

jurisdictions that offer offshore financial services. Casinos, including internet casinos, are illegal in Ireland. Private gaming clubs, however, operate casino-like facilities that fall outside the scope of the law.

Ireland criminalized money laundering relating to narcotics trafficking and all indictable offenses under the 1994 Criminal Justice Act. Financial institutions (banks, building societies, the Post Office, stockbrokers, credit unions, bureaux de change, life insurance companies, and insurance brokers) are required to report suspicious transactions. There is no monetary threshold for reporting suspicious transactions. Designated entities submit suspicious transaction reports (STRs) to the Garda (Irish Police) Bureau of Fraud Investigation, Ireland's Financial Intelligence Unit (FIU). In 2003, a new legal requirement went into effect, mandating that covered institutions file STRs with the Revenue (Tax) Department in addition to the FIU.

Financial institutions are required to implement customer identification procedures and retain records of financial transactions. In 2003, Ireland amended its Anti-Money Laundering law to extend the requirements of customer identification and suspicious transaction reporting to lawyers, accountants, auditors, real estate agents, auctioneers, and dealers in high-value goods, thus aligning its laws with the Second European Union (EU) Money Laundering Directive. Ireland's Customer Due Diligence requires designated entities to take measures to identify customers when opening new accounts or conducting transactions exceeding 13,000 euros (approximately $17,000). These requirements do not extend to existing customers prior to May 1995 except in cases where authorities suspect that money laundering or another financial crime is involved.

The Corporate Law, amended in 1999, requires that every company applying for registration in Ireland must demonstrate that it intends to carry on an activity in the country. Companies must maintain an Irish resident director at all times, or post a bond as a surety for failure to comply with the appropriate company law. In addition, the law limits the number of directorships that any one person can hold to 25, with certain exemptions. This limitation aims to curb the use of nominee directors as a means of disguising beneficial ownership or control.

The Company Law Enforcement Act 2001 (Company Act) established the Office of the Director of Corporate Enforcement (ODCE). The ODCE investigates and enforces provisions of the Company Act. Under the law, directors of a company must be named, and the ODCE has power to establish the company's beneficial ownership and control. The Company Act also creates a mandatory reporting obligation for auditors to report suspicions of breaches of company law to the ODCE. In 2005, the ODCE secured the conviction of 30 company directors and other individuals on 49 charges for breaching various requirements of the Company Act. In addition, 21 company officers were disqualified from eligibility for a lead position in companies for periods ranging from one to 10 years.

The Third EU Money Laundering Directive entered into force in December 2005 and must be transposed into Irish law by December 2007. The Government of Ireland (GOI) is likely to implement new legislation to address customer due diligence, the identification of beneficial owners, politically exposed persons, and the designation of trusts.

A Mutual Evaluation conducted in 2005 by the Financial Action Task Force (FATF) which was published in 2006 noted that Ireland's money laundering definition met the FATF requirements. The mutual evaluation report (MER) acknowledged that Ireland achieved a high standing in anti-money laundering legal structures and international cooperation, although the number of money laundering prosecutions and convictions was low.

The Irish Financial Services Regulatory Authority (IFSRA), the financial regulator, is a component of the Central Bank and Financial Services Authority of Ireland (CBFSAI) and is responsible for supervising the financial institutions for compliance with money laundering procedures. IFSRA is obliged to report to the FIU and the Revenue Commissioners regarding any suspected breaches of the

Criminal Justice Act 1994 by the institutions under its supervision. Such reports cover suspicion of money laundering and terrorism financing, failure to establish identity of customers, failure to retain evidence of identification, and failure to adopt measures to prevent and detect the commission of a money laundering offense. IFSRA regulates the IFSC companies that conduct banking, insurance, and fund transactions. Tax privileges for IFSC companies were phased out over recent years and expired in 2005.

Ireland currently has no legislative requirement to report cross-border transportation of currency or bearer-negotiable instruments, although reportedly the government is likely to introduce customs reporting requirements in 2007 for those transporting more than euro 10,000 (approximately $12,900) into or out of the EU. In addition, movements of gold, precious metals, and precious stones into or out of the EU when Ireland is the initial entry or final exit point must be reported to Irish Customs. The FIU will have access to these reports.

Ireland estimates that up to 80 percent of STRs may involve tax violations. Value Added Tax (VAT) Intra-Community Missing Trader Fraud is extensive within the EU, and there is evidence in several fraud investigations that conduit traders involved in the supply chain have been established in Ireland. This particular fraud is a systematic criminal attack on the VAT system, detected in many EU countries, in which criminals obtain VAT registration to acquire goods VAT free from other Member States. They then sell on the goods at VAT inclusive prices and disappear without remitting the VAT paid by their customers to the tax authorities.

Ireland's FIU analyzes financial disclosures, and disseminates them for investigation. There are no legal provisions, however, governing the time period within which an STR must be filed; rather, the requirement is to submit the STR before a suspicious transaction is finalized. The MER found that Ireland's FIU, as a whole, met the requirements of the FATF methodology, but had limited technical and human resources to manage and evaluate STRs effectively.

In 2005, the FIU received 10,735 STRs, in comparison with 5,491 in 2004 and 4, 254 in 2003. 2005 saw eight prosecutions for money laundering and three convictions. In 2006, three people were convicted for money laundering. A conviction on charges of money laundering carries a maximum penalty of 14 years' imprisonment and an unlimited fine. The lengthiest penalty applied for a money laundering conviction to date has been six years. Under certain circumstances, the High Court can freeze, and, where appropriate, seize the proceeds of crimes.

The Criminal Assets Bureau (CAB) was established in 1996 to confiscate the proceeds of crime in cases where there is no criminal conviction. The CAB reports to the Minister for Justice and includes experts from the Garda, Tax, Customs, and Social Security Agencies. Under the 1996 Proceeds of Crime Act, specified property valued in excess of 13,000 euro (approximately $17,000) may be frozen for seven years, unless the court is satisfied that all or part of the property is not criminal proceeds. In February 2005, the Proceeds of Crime (Amendment) Act 2005 came into effect, enabling the authorities, with the consent of the High Court and the parties concerned, to dispose of assets without having to await the expiry of seven years. To date, the authorities have executed five such consent orders. This Act also allows foreign criminality to be taken into account in assessing whether assets are the proceeds of criminal conduct. In 2005, the CAB obtained final and interim restraint orders on assets valued at approximately $76 million. The Proceeds of Crime (Amendment) Act 2005 has a specific provision that allows the CAB to cooperate with agencies in other jurisdictions, which should strengthen Irish cooperation with asset recovery agencies in the UK, including Northern Ireland.

In March 2005, the Irish government enhanced its capacity to address international terrorism with the enactment of the Criminal Justice (Terrorism Offenses) Act. This legislation brought Ireland in line with United Nations Conventions and European Union Framework decisions on combating terrorism. In addition, the IFSRA works with the Department of Finance to draft guidance for regulated institutions on combating and preventing terrorist financing. The authorities revised and issued the

guidance to institutions upon the passage of the Criminal Justice Act in 2005. Implementation of the new antiterrorism legislation and its anti-money laundering law amendments, in addition to stringent enforcement of all such initiatives, should enhance Ireland's efforts to maintain an effective anti-money laundering program.

To date, there have been no prosecutions for terrorism offenses under the Criminal Justice Act. The 2006 FATF MER noted that the Act neglects to cover funding of either a terrorist acting alone or two terrorists acting in concert. The MER also noted inadequate implementation of UN Security Council Resolution (UNSCR) 1373, in that Ireland relies exclusively on an EU listing system without subsidiary mechanisms to deal with terrorists on the list who are European citizens (the EU Regulations do not apply for freezing purposes to such persons) or with persons designated as terrorists by other jurisdictions who are not on the EU list. The Criminal Justice (Terrorism Offenses) Act imposes evidentiary requirements contrary to obligations under UNSCR 1373 to freeze all funds and assets of individuals who commit terrorist acts, whether or not there is evidence that those particular funds are intended for use in terrorist acts.

The Garda can apply to the courts to freeze assets when certain evidentiary requirements are met. From 2001 through 2006, Ireland had reported to the European Commission the names of five individuals (most recently in 2004) who maintained a total of seven accounts that were frozen in accordance with the provisions of the European Union's (EU) Anti-Terrorist Legislation. The aggregate value of the funds frozen was approximately $6,400.

In July 2005, the United States and Ireland signed instruments on extradition and mutual legal assistance. These instruments are part of a sequence of bilateral agreements that the United States is concluding with all 25 EU Member States, in order to implement twin agreements on extradition and mutual legal assistance with the European Union that were concluded in 2003. The instruments signed by Ireland supplement and update the 1983 U.S.-Ireland extradition treaty and the 2001 bilateral treaty on mutual legal assistance (MLAT). The 1983 extradition treaty between Ireland and the U.S. is in force, while the ratification process for the 2001 MLAT has not yet been completed by the GOI. In November 2006, Ireland extradited a U.S. citizen, the first successful case in the last eighteen requests. The new MLAT instrument signed in July 2005 provides for searches of suspect foreign located bank accounts, joint investigative teams, and testimony by video-link.

Ireland is a member of the FATF, and its FIU is a member of the Egmont Group. Ireland is a party to the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, and the 1988 UN Drug Convention.

The GOI should enact legislation to disallow the establishment of "shell" companies. Law enforcement should have a stronger role in identifying the true beneficial owners of shell companies as well as of trusts in the course of investigations. Ireland should increase the technical and human resources provided to the FIU in order to manage and evaluate STRs effectively. The GOI should enact legislation that covers funding of a terrorist acting alone and funding of two terrorists acting in concert, as well as legislation fully implementing UNSCR 1373. To this end, Ireland should remove the evidentiary requirements acting as obstacles to full compliance, as well as circulate the UN and the U.S. lists to its regulators and obligated entities.

Isle of Man

The Isle of Man (IOM) is a Crown Dependency of the United Kingdom located between England and Ireland in the Irish Sea. Its large and sophisticated financial center is potentially vulnerable to money laundering. The U.S. dollar is the most common currency used for criminal activity in the IOM. Most of the illicit funds in the IOM are from fraud schemes and narcotics trafficking in other jurisdictions,

including the United Kingdom. Identity theft and Internet abuse are growing segments of financial crime activity.

Money laundering related to narcotics trafficking was criminalized in 1987. 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. In 1998, money laundering arising from all serious crimes was criminalized. Financial institutions and professionals such as banks, fund managers, stockbrokers, insurance companies, investment businesses, credit unions, bureaux de change, check cashing facilities, money transmission services, real estate agents, auditors, casinos, accountants, lawyers, and trustees are required to report suspicious transactions and comply with the requirements of the anti-money laundering (AML) code, such as customer identification.

The Financial Supervision Commission (FSC) and the Insurance and Pension Authority (IPA) regulate the IOM financial sector. 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 IPA regulates insurance companies, insurance management companies, general insurance intermediaries, and retirement benefit schemes and their administrators. In addition, 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.

Instances of failure to disclose suspicious activity would result in both a report being made to the Financial Crimes Unit (FCU), the IOM's financial intelligence unit (FIU), and possible punitive action by the regulator, which could include revoking the business license. To assist license holders in the effective implementation of anti-money laundering techniques, the regulators hold regular seminars and additional workshop training sessions in partnership with the FCU and the Isle of Man Customs and Excise.

In December 2000, the FSC issued a consultation paper, jointly with the Crown Dependencies of Guernsey and Jersey, called Overriding Principles for a Revised Know Your Customer Framework, to develop a more coordinated approach on anti-money laundering. Further work between the Crown Dependencies is being undertaken to develop a coordinated strategy on money laundering, to ensure compliance as far as possible with the revised Financial Action Task Force (FATF) Forty Recommendations on Money Laundering. The IOM is also assisting the FATF Working Groups considering matters relating to customer identification and companies' issues.

In August 2002, money service businesses (MSBs) not already regulated by the FSC or IPA were required to register with Customs and Excise. This implemented the 1991 EU Directive on Money Laundering, revised by the Second Directive 2001/97/EC, for MSBs and provides for their supervision by Customs and Excise to ensure compliance with the AML Codes.

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 the Overriding Principles. These include a requirement that all insurance businesses check their whole book of businesses to determine that they have sufficient information available to prove customer identity. The current set of Standards became effective March 31, 2003. In addition, 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 more detailed guidance on the prevention of money laundering through the use of online gambling. The Online Gambling legislation brought regulation to what was technically an unregulated gaming environment. The dedicated Online Gambling AML Code was at the time unique within this segment of the gambling industry.

The Companies, Etc. (Amendment) Act 2003 calls for additional supervision for all licensable businesses, e.g., banking, investment, insurance and corporate service providers. The act further provides that no future bearer shares will be issued after April 1, 2004, and all existing bearer shares must be registered before any rights relating to such shares can be exercised.

The FCU, formed in April 2000, evolved from the police Fraud Squad and now includes both police and customs staff. It is the central point for the collection, analysis, investigation, and dissemination of suspicious transaction reports (STRs) from obligated entities. The entities required to report suspicious transactions include banks/financial institutions, bureaux de change, casinos, post offices, lawyers, accountants, advocates, and businesses involved with investments, real estate, gaming/lotteries, and insurance. In 2006, the FIU received approximately 1,625 suspicious transaction reports (STRs); in 2005 the FIU received 2,265 STRs and in 2004 it received 2,315 STRs. In 2006, the FIU referred approximately 16 percent of the STRs to the United Kingdom, 10 percent to other European jurisdictions and 15 percent to non-European jurisdictions as referrals to law enforcement for investigation. The Isle of Man's International Co-operation team responded to 70 letters of request (from January to November 2006), under Mutual Legal Assistance Treaties (MLATs). The International Co-operation team responded to 103 requests for information in 2005 and 115 requests in 2004. There is no minimum threshold for obligated entities to file a STR and reporting individuals (compliance officers, bankers, etc.) are protected by law when filing suspicious transactions.

The FCU is organized under the Department of Home Affairs. The FIU has access to Customs, police and tax information. The STRs are disseminated through agreements to the IOM Customs, Tax Administrators, Financial Supervision Commission (FSC) and the Insurance and Pension Authority (IPA). The FCU is responsible for investigating financial crimes and terrorist financing cases. In 2006, there were two individuals charged for money laundering offences involving narcotics. The FCU also has three additional investigations on-going relating to money laundering offences involving fraud.

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. Assistance by way of restraint and confiscation of assets of a defendant is available under the 1990 Act to all countries and territories designated by Order under the Act, and the availability of such assistance is not convention-based nor does it require reciprocity. 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.

Under the 1990 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. The law also addresses the disclosure of a suspicion of money laundering. Since June 2001, it has been an offense to fail to make a disclosure of suspicion of money laundering for all predicate crimes, whereas previously this just applied to drug- and terrorism-related crimes. 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. The law also 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 United Kingdom implemented the amendments to its Proceeds of Crime Act in 2004. The IOM is currently reviewing new legislation that will revise its Criminal Justice Act along similar lines. The new amendments are under consideration and are expected to come into force in 2007.

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 Government of the IOM enacted the Anti-Terrorism and Crime Act, 2003. The purpose of the Act is to enhance reporting, by making it an offense not to report suspicious transactions relating to money intended to finance terrorism. The IOM Terrorism (United Nations Measure) Order 2001 implements UNSCR 1373 by providing for the freezing of terrorist funds, as well as by creating a criminal offense with respect to facilitators of terrorism or its financing. All charities are registered and supervised by the Charities Commission. 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. The FSC's anti-money laundering guidance notes have been revised to include information relevant to terrorist events. The Guidance Notes were issued in December 2001. Additional amendments are being reviewed that will incorporate the new FATF recommendations and EU directives.

The IOM has developed a legal and constitutional framework for combating money laundering and the financing of terrorism. There appears to be a high level of awareness of anti-money laundering and counterterrorist financing issues within the financial sector, and considerable effort has been made to put appropriate practices into place. In November 2003, the Government of the IOM published the full report made by the International Monetary Fund (IMF) following its examination of the regulation and supervision of the IOM's financial sector. In this report the IMF commends the IOM for its robust regulatory regime. The IMF found that "the financial regulatory and supervisory system of the Isle of Man complies well with the assessed international standards." The report concludes the Isle of Man fully meets international standards in areas such as banking, insurance, securities, anti-money laundering, and combating the financing of terrorism.

The IOM is a member of the Offshore Group of Banking Supervisors. The IOM is also a member of the International Association of Insurance Supervisors and the Offshore Group of Insurance Supervisors. The FCU belongs to the Egmont Group. The IOM cooperates with international anti-money laundering authorities on regulatory and criminal matters. Application of the 1988 UN Drug Convention was extended to the IOM in 1993.

Isle of Man officials should continue to support and educate the local financial sector to help it combat current trends in money laundering. The authorities should continue to protect the integrity of the Island's financial system by aggressively identifying, investigating, and prosecuting those involved with money laundering and other financial crimes. The Isle of Man should continue to work with international anti-money laundering authorities to deter financial crime and the financing of terrorism and terrorists.

Israel

Despite its relatively high GDP, per capita income, and developed financial markets, Israel is not 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. Reportedly, less than a quarter of all Israeli money laundering or terrorist financing seizures are related to narcotics proceeds. The majority of the seizures are related to fraud, theft, embezzlement, and illegal money services providers (MSP). Most financial crime investigations in 2006 were related to the intentional failure to report major financial transactions, or the falsification of transaction reports—particularly property transactions. 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 more than 18 serious crimes, in addition to offenses described in the prevention of terrorism ordinance, as predicate offenses for money laundering.

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. The PMLL requires 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 $17,200). 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. This offense is punishable by up to six months imprisonment or a fine of NIS 202,000 (approximately $43,400), or ten times the amount that was not declared, whichever is higher. Alternatively, an administrative sanction of NIS 101,000 (approximately $21,700), or five times the amount that was not declared, may be imposed. In 2003, the Government of Israel (GOI) lowered the threshold for reporting cash transaction reports (CTRs) to NIS 50,000 (approximately $10,500), lowered the document retention threshold to NIS 10,000 (approximately $2,100), and imposed more stringent reporting requirements.

The PMLL also provided for the establishment of the Israeli Money Laundering Prohibition Authority (IMPA), 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. The term "unusual transactions" is loosely defined. However, it is used so that the IMPA will receive reports even when the financial institution is unable to link the unusual transaction with money laundering. In addition, suspicious transaction reporting is required of 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. The PMLL does not apply to intermediaries, such as lawyers and accountants.

In 2002, Israel enacted several new amendments to the PMLL that resulted in the addition of the money services businesses (MSB) to the list of entities required to file cash transaction reports (CTRs) and suspicious transaction reports (STRs), 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, and the creation of rules on safeguarding the IMPA database and rules for requesting and transmitting information between IMPA, the Israeli National Police (INP) and the Israel Security Agency (Shin Bet). The PMLL also authorized the issuance of regulations requiring financial service providers to identify, report, and keep records for specified transactions for seven years.

In April 2006, the Justice Ministry proposed an amendment to the PMLL that extends Israel's Anti-Money Laundering (AML) regime to cover its substantial diamond trading industry. The amendment defines "dealers in precious stones" as those merchants whose annual transactions reach NIS 50,000 (approximately $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 maintain all transaction records and client identification for at least five years. This proposal has not yet been passed into legislation by the Knesset.

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. The Banking Order was expanded to cover the prohibition on financing terrorism to include obligations to check the identification of parties to a transaction against declared terrorists and terrorist organizations, as well as obligations of reporting by size and type of transaction. The Banking Order sets the minimum size of a transaction that must be reported at NIS 5,000 (approximately $1,180) 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.

Another new regulation added in 2006 allows the INP and the Shin Bet to use information provided to them by IMPA to investigate other offenses in addition to money laundering and terror financing. 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 in order to avoid its abuse and to set guidelines for the police and security services. Other legislative initiatives passed in 2006 include provisions to the Combating Criminal Organizations Law, which applies forfeiture and seizure provisions to criminal offenses resulting from trafficking-in-persons.

The PMLL mandates the registration of MSBs through the Providers of Currency Services Registrar at the Ministry of Finance. In 2004, Israeli courts convicted several MSBs for failure to register with the Registrar of Currency Services. In addition, several criminal investigations have been conducted against other currency-services providers, some of which have resulted in money laundering indictments, which are still pending. The closure of unregistered MSBs remained a priority objective of the INP in 2006. 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. In the past year, Israeli courts convicted several MSBs for violating the obligation to register with the Registrar of Currency Services. In addition, several criminal investigations were brought against other MSBs, some of which resulted in money laundering indictments that are still pending criminal trials.

The INP reports no indications of an overall increase in financial crime relative to previous years. In 2006, IMPA reported 77 arrests and five prosecutions relating to money laundering and/or terrorist financing. In one of this year's major AML operations, the INP arrested three senior employees of the Mercantile Discount Bank branch in Ramleh, as well as 23 customers, under suspicion of conspiring to launder tens of millions of shekels earned from extortion and gambling. Another extensive investigation revealed an organized criminal operation that had gained control over several gas stations in the greater Jerusalem area, and was diluting gasoline with other liquids in order to increase profits. The investigation resulted in 12 arrests, property seizures, and an indictment against 28 defendants for filing fictitious invoices amounting to NIS 350 million, and money laundering among other offenses. IMPA reported six other large criminal cases in 2006 totaling over NIS 160 million (approximately $37,749,310) in laundered money.

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. 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.

Israeli authorities regularly distribute the names of individuals and entities on the UNSCR 1267 Sanctions Committee consolidated list.

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. The identification and tracing of such assets is part of the ongoing function of the Israeli intelligence authorities and IMPA. In 2006, IMPA received 9,400 suspicious transaction reports. During this period IMPA disseminated 384 intelligence reports to law enforcement agencies and to foreign FIUs in response to requests, and on its own initiative. In addition, twelve different investigations yielded indictments (some of them multiple indictments). In another case, prosecutors indicted a number of bank officials for money laundering offenses for violation of the obligation to report unusual transactions and for advising their customers on ways of avoiding reporting to IMPA. In 2006, the INP seized approximately $12 million in suspected criminal assets, a significant decrease from the $75 million seized in 2005. Total seizures for each of the previous three years ranged from $23-$27 million each year.

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. Israel has signed but not yet ratified the UN Convention against Corruption. Israel is also in the final stages of domestic approval for its accession to the Second Additional Protocol to the Council of Europe Convention, 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.

The Government of Israel continues to make progress in strengthening its anti-money laundering and terrorist financing regime in 2006. 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.

Italy

Italy is not an offshore financial center. Italy is part of the euro area and 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, and Russia.

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 myriad criminal activities, such as alien smuggling, contraband cigarette smuggling, pirated goods, extortion, usury, and kidnapping. Financial crimes not directly linked to money laundering, such as credit card and Internet fraud, are increasing.

Money laundering occurs both in the regular banking sector and in the nonbank financial system, including in 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. Italy's underground economy in 2002 was an estimated 27 percent of Italian GDP, or approximately 200 billion euros.

According to a 2006 IMF evaluation, Italy's anti-money laundering and counterterrorist 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. Banks must identify their customers and record any transaction that exceeds 12,500 euros (approximately $15,000). 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—must be reported on a case-by-case basis. Italian law prohibits the use of cash or negotiable bearer instruments for transferring money in amounts in excess of approximately $15,000, 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 $15,000-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. In any event, financial institutions are required to maintain a uniform anti-money laundering database for all transactions (including wire transfers) over $15,000 and to submit this data monthly to the Italian Exchange Office (known in Italian as 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 2005, the UIC received 8,576 suspicious transaction reports (STRs) related to money laundering and 482 related to terrorism finance. 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 per cent of all STRs. Money remittance operators submit 13.5 per cent of the total number of STRs, and all other sectors together account for less than ten per cent.

The UIC, which is an arm of the Bank of Italy (BoI), receives and analyzes STRs filed by covered institutions, and then forwards 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 which carry on activities that could be exposed to money laundering. The UIC has access to the banks' customer database. 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 performs 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. STRs helped lead the GdF to identify $14,400,000 in laundered money in 2003.

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 euro 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 have been frozen belonging to 55 persons, totaling $528,000 under United Nations resolutions relating to terrorist financing. 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 as part of criminal investigation of crimes linked to international terrorism or by applying administrative seizing 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 and to issue provisions to make more effective the freezing of nonfinancial assets belonging to listed terrorist groups and individuals.

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 per se. Primarily for tax purposes, in 1997 Italy created a category of "not-for-profit organizations of social utility" (ONLUS). Such organizations can be associations, foundations or fundraising committees. To be classified as an ONLUS, the organization must register with the Finance Ministry and prepare an annual report. There are currently 19,000 registered entities in the ONLUS category.

Established in 2000, the ONLUS Agency issues guidelines and drafts legislation for the nonprofit sector, alerts other authorities of violations of existing obligations, and confirms de-listings from the ONLUS registry. The ONLUS Agency cooperates with the Finance Ministry in reviewing the 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 terrorism 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 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, and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. Italy ratified the UN Convention against Transnational Organized Crime with the passage of Law no. 146 of March 16, 2006.

Italy is a member of the Financial Action Task Force (FATF) and held the FATF presidency in 1997-98. As a member of the Egmont Group, Italy's UIC shares information with other countries' FIUs. The UIC has been authorized to conclude information-sharing agreements concerning suspicious financial transactions with other countries. To date, Italy has signed memoranda of understanding with France, Spain, the Czech Republic, Croatia, Slovenia, Belgium, Panama, Latvia, the Russian Federation, Canada, and Australia. Italy also is negotiating agreements with Japan, Argentina, Malta, Thailand, Singapore, Hong Kong, Malaysia, and Switzerland. Italy has a number of bilateral agreements with foreign governments in the areas of investigative cooperation on narcotics trafficking and organized crime. 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 fora 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. Because of its location as a major transit center for cocaine, payments for drugs pass through Jamaica in the form of cash shipments back to South America. The profits from these heavy illegal drug flows must be legitimated and therefore make Jamaica susceptible to money laundering activities and other financial crimes. In 2006, 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.

Jamaica is neither an offshore financial center, nor is it a major money laundering country. The Government of Jamaica (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. 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. Jamaican banking authorities do not license offshore banks or other forms of exempt or shell companies. However, nominee or anonymous directors and trustees are allowed for companies registered 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. 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.

The two free trade zones that operate in Jamaica are in Montego Bay and Kingston. Due to the demise of the garment industry, the Kingston Free Zone is essentially dormant and only a small amount of warehouse space remains. The Montego Bay Free Zone has a small cluster of information technology companies. There is no indication that either free zone is being used for trade-based money laundering or terrorist financing. There is one gaming entity operating in the free zone; its license does not permit local betting. Domestic casino gambling is permitted in Jamaica.

The Money Laundering Act (MLA), as amended in February 2000, currently governs Jamaica's anti-money laundering regime. The MLA criminalizes money laundering related to narcotics offenses, fraud, firearms trafficking and corruption. Bank secrecy laws exist; however, there are provisions under GOJ law to enable law enforcement access to banking information.

Under the MLA, banks and a wide range of financial institutions (including wire-transfer companies, exchange bureaus, building societies, insurance companies and securities dealers) are required to report suspicious transactions of any amount to Jamaica's financial intelligence unit, the Financial Investigations Division (FID) of the Ministry of Finance. The MLA establishes a five-year record-keeping requirement and requires financial institutions to report all currency transactions over

$50,000. Exchange bureaus have a reporting threshold of $8,000. Jamaica's central bank, the Bank of Jamaica, supervises the financial sector for compliance with anti-money laundering provisions.

The FID has operated as the de facto FIU since 2001. Under the draft Proceeds of Crime Act, which is currently being debated before Parliament, the FID will be named as Jamaica's official FIU. Companion legislation to the Act has been drafted to allow the sharing of information with other FIUs. In preparation for its expanded investigative role once the Act is passed, the FID has embarked on a five-stage plan to enhance its capacity in 2006. This includes the installation of a new computer system to process and track cases.

The FID consists of 14 forensic examiners, six police officers who have full arrest powers, a director and five administrative staff. Suspicious transaction reports (STRs) or cash transaction reports (CTRs) that are deemed to warrant further investigation are referred to the Financial Intelligence Division within the FID. Efforts are underway to improve the cooperation between the Tax authorities (TAAD) and the FID. Both the FID and the TAAD units suffer from a lack of adequate resources; therefore, the TAAD's competing priorities—such as revenue collection obligations, a main focus of the GOJ—take precedence over assisting the FID with money laundering investigations.

Jamaica has an ongoing education program to ensure compliance with the mandatory STR requirements. Reporting individuals are protected by law with respect to their cooperation with law enforcement entities. The FID reports that nonbanking financial institutions have a 70 percent compliance rate with money laundering controls. In 2006, 18,311 STRs were filed; of these, 14 were referred to law enforcement for investigation. Since January 2006, seven persons have been arrested and charged with money laundering.

The Jamaican Parliament's 2004 amendments to the Bank of Jamaica Act, the Banking Act, the Financial Institutions Act, and the Building Societies Act improved the governance, examination and supervision of commercial banks and other financial institutions by the Bank of Jamaica. Amendments were also passed to the Financial Services Commission Act, which governs financial entities supervised by the Financial Services Commission. These measures expanded 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 the foundation to complement the proposed reforms to the MLA through the enactment of the draft Proceeds of Crime Act.

The GOJ requires customs declaration of currency or monetary instruments over $10,000 (or its equivalent). The Airport Interdiction Task Force, a joint law enforcement effort by the United States, United Kingdom, Canada and Jamaica, will begin operation in early 2007. The Task Forces 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.

Currently, the FID and the Jamaica Constabulary Force (JCF) are the entities responsible for tracing and seizing assets. Law enforcement authorities are hampered by the fact that Jamaica has no civil forfeiture law. Under the 1994 Drug Offenses (Forfeiture of Proceeds) Act, a criminal drug-trafficking conviction is required prior to forfeiture. This often means that even when police discover illicit funds, the money cannot be seized or frozen and must be returned to the criminals. Assets that are eventually forfeited are deposited into a fund shared by the Ministries of National Security, Justice and Finance.

The Proceeds of Crime Act, when passed, would incorporate the existing provisions of the MLA and would allow for the civil forfeiture of assets related to criminal activity. The Act would expand the confiscation powers of the GOJ and permit, upon conviction, the forfeiture of benefits assessed to have been received by the convicted party within the six years preceding the conviction. The Act would include a provision allowing for the forfeiture of assets related to human trafficking and terrorist financing, and would apply 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. Under the Act, the proposed division of forfeited assets would distribute one-third of assets to the Ministry of National Security, one-third to the Ministry of Finance, and one-third to the Ministry of Justice.

There was an increase in the amount of both seizures and forfeitures of assets for 2006. In 2006, over $2 million was seized and $1.5 million was forfeited, a significant increase over the $646,000 seized and $476,000 forfeited in 2005. Nondrug related assets go to a consolidated or general fund, while drug related assets—which totaled $560,000 in 2006—are placed into a forfeited asset fund, which benefits law enforcement.

The draft Proceeds of Crime Act addresses many of the shortcomings of the GOJ's current legislative anti-money laundering and asset forfeiture regime. However, despite a lack of major opposition to the bill, the Act has been under consideration for a year. The GOJ intends to pass the Act in early 2007.

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.

The GOJ has not encountered any misuse of charitable or nonprofit entities as conduits for the financing of terrorism. The Ministry of Finance is currently finalizing its risk-assessment report on charitable organizations.

Jamaica and the United States have a Mutual Legal Assistance Treaty that entered into force in 1995. 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. The FID is not a member of the Egmont Group of financial intelligence units.

The Government of Jamaica should ensure the swift passage of legislation to improve its anti-money laundering efforts, as well as procedures to enhance asset forfeiture. Jamaica should ensure that the proposed legislative reforms allow for a fully functioning financial intelligence unit that meets the membership criteria of the Egmont Group and other international standards. A more aggressive effort is necessary to bring Jamaica's anti-money laundering and counterterrorist financing regime into line with international standards.

Japan

Japan is the world's second largest economy and a large and 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, 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. The number of Internet-related money laundering cases involving Japan is also increasing. In some cases, criminal proceeds were concealed in bank accounts obtained through an Internet market. Laws enacted in 2004 make online sales of bank accounts illegal.

On November 17, 2005, the Japanese government's headquarters for the Promotion of Measures against Transnational Organized Crime and Other Related Issues and the headquarters for International Terrorism agreed that relevant ministries would submit a bill to the 2007 ordinary session of the Diet to enhance compliance with the FATF Forty Recommendations and the FATF Nine Special Recommendations on Terrorist Financing. It is now expected that these recommendations will be promulgated by April 1, 2007, given the probable timing for the Anti-Money Laundering Law currently being drafted by the National Police Agency. In accordance with the FATF Forty Recommendations of 2003, the new Anti-Money Laundering Law will include a wider range of sectors required to submit suspicious transaction reports (STR), including accountants, real estate agents, dealers in precious metals and stones, and certain types of company service providers. The government of Japan is also considering measures to implement the FATF's Special Recommendation Nine, which recommends cross-border currency reporting requirements.

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. It also authorizes electronic surveillance of organized crime members, and enhances the suspicious transaction reporting system.

The AOCL was partially revised in June of 2002 by the "Act on Punishment of Financing to Offences of Public Intimidation," which specifically added the financing of terrorism to the list of money laundering predicates. An amendment to the AOCL was submitted on February 20, 2004 to the Diet for approval, was resubmitted to the Diet in October 2005, and remains under consideration. The amendment would expand the predicate offenses for money laundering from approximately 200 offenses to nearly 350 offenses, with almost all offenses punishable by imprisonment.

Japan's Financial Services Agency (FSA) supervises public-sector 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. Financial institutions in Japan forward STRs to JAFIO, which analyzes and disseminates them as appropriate. At the end of 2005, Japan announced plans to transfer JAFIO from the FSA to the National Policy Agency, possibly on April 1, 2007, pending the successful passage of the new Anti-Money Laundering Law.

In 2006, JAFIO 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, JAFIO disseminated to law enforcement 71,241 STRs, up from 66,812 STRs disseminated in 2005.

JAFIO concluded international cooperation agreements during 2006 with the FIU's of Australia, Thailand, Hong Kong, Canada and Indonesia. In 2004, JAFIO concluded such cooperation agreements with Singapore's Financial Intelligence Unit (FIU) and with FinCEN, establishing cooperative frameworks for the exchange of financial intelligence related to money laundering and terrorist financing. JAFIO already had similar agreements in place with the FIUs of the United Kingdom, Belgium, and South Korea. 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. In 2003, the United States and Japan concluded a Mutual Legal Assistance Treaty (MLAT).

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 protects 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 also revised so that financial institutions are required to make positive customer identification for both domestic transactions and transfers abroad in amounts of more than two million yen (approximately $16,950). Banks and financial institutions are required to maintain customer identification records for seven years.

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 $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. 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 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.

Underground banking systems operate widely in Japan, especially in immigrant communities. Such systems violate the Banking Law and the Foreign Exchange 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 joined the Egmont Group of FIUs in 2000. Japan is also a member of the Asia/Pacific Group against Money Laundering. In 2002, Japan's FSA and the U.S. Securities and Exchange Commission and Commodity Futures Trading Commission signed a nonbinding Statement of Intent (SOI) concerning cooperation and the exchange of information related to securities law violations. In January 2006 the FSA and the U.S. SEC and CFTC signed an amendment to their SOI to include financial derivatives.

The government of Japan has many legal tools and agencies in place to successfully detect, investigate, and combat money laundering. In order to strengthen its money laundering regime, Japan should stringently enforce the Anti-Organized Crime Law. Japan should also enact penalties for noncompliance with 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, 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.

Jersey

The Bailiwick of Jersey (BOJ) encompasses part of the Channel Islands and is a Crown Dependency of the United Kingdom. The majority of illicit money in Jersey is derived from foreign criminal activity. Local drug trafficking and corruption of politically exposed persons (PEP) are sources of

illicit proceeds found in the country. Jersey's sophisticated array of offshore services is similar to that of international financial services centers worldwide. Money laundering mostly occurs with Jersey's banking system, investment companies, and local trust companies. As of September 2006, the financial services industry consists of 47 banks, 908 trust companies, 175 insurance companies (largely captive insurance companies), and 1086 collective investment funds. Other services include investment advice, dealing, and management companies, and mutual fund companies. In addition the 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 many wealth management services.

The International Monetary Fund (IMF) conducted an assessment of the anti-money laundering regime of Jersey in October 2003. The IMF team found Jersey's Financial Services Commission (JFSC), the financial services regulator, to be in compliance with international standards, but provided recommendations for improvement.

The Jersey Finance and Economics Committee administers the law regulating, supervising, promoting, and developing the Jersey finance industry. The IMF report noted that the Finance and Economics Committee's power to give direction to the JFSC might appear to be a conflict of interest between the two agencies, and suggested that the BOJ establish a separate body to speak for the industry's consumers. The report proposed that Jersey authorities establish rules for banks dealing with market risk, along with a code of conduct for collective investment funds. The IMF report also recommended that the BOJ institute a contingency plan for the failure of a major institution.

Jersey is working to address the issues raised in the report. The JFSC reportedly intends to continue to strengthen its existing regulatory powers and amend the Financial Services Commission Law 1998 to provide legislative support for its inspections. The JFSC also plans to introduce monetary fines for administrative and regulatory breaches. Improvements will also include stricter industry guidelines and tighter enforcement of anti-money laundering and terrorist financing controls.

Jersey's main anti-money laundering 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 broadens the predicate offenses for money laundering to all offenses punishable by at least one year in prison. The Prevention of Terrorism (Jersey) Law 1996, which criminalizes money laundering related to terrorist activity, was replaced by the Terrorism (Jersey) Law 2002 that came into force in January 2003. The Terrorism (Jersey) Law 2002 is a response to the events of September 11, 2001, and enhances the powers of BOJ authorities to investigate terrorist offenses, to cooperate with law enforcement agencies in other jurisdictions, and to seize assets. Jersey passed the Corruption Law 2005 in alignment with the Council of Europe Criminal Law Convention on Corruption. Although the law was registered in May 2006, by the end of 2006 it had not yet come into force.

Suspicious transaction reporting is mandatory under the narcotics trafficking, terrorism, and anti-money laundering laws. There is no threshold for filing a suspicious transaction report, and the reporting individual is protected from criminal and civil charges by safe harbor provisions in the law. Record keeping requirements mandate that banks and other financial service companies maintain financial records of their customers for a minimum of 10 years. The JFSC has issued anti-money laundering (AML) Guidance Notes that the courts consider when determining whether or not an offense has been committed under the Money Laundering Order. Penalties for a money laundering conviction include imprisonment for a minimum of one year.

After consultation with the financial services industry, the JFSC issued a joint paper with Guernsey and the Isle of Man that recommended proposals to tighten the essential due diligence requirements for financial institutions with regard to their customers. The position paper states the JFSC's insistence on the responsibility of all financial institutions to verify the identity of their customers, regardless of

any intermediary. The paper also outlines a program to obtain verification documentation for customer relationships preceding the Proceeds of Crime (Jersey) Law. Working groups review specific portions of these principles annually and draft AML Guidance Notes to incorporate changes and improvements.

Approximately 31,162 Jersey companies are registered with the Registrar of Companies. In addition to public filings relating to shareholders, the JFSC requires each Jersey-registered company to file details regarding the ultimate beneficial owners. That information is held confidentially but is available to domestic and foreign investigators under appropriate circumstances and in accordance with the law.

A number of companies registered in other jurisdictions are administered in Jersey. "Exempt companies" do not pay Jersey income tax and are only available to nonresidents. Jersey does not provide offshore licenses. All financial businesses must have a presence in Jersey and their management must be located in Jersey. Alternate remittance systems reportedly are not prevalent.

Jersey has established a Financial Intelligence Unit (FIU) known as the Joint Financial Crime Unit (JFCU). This unit receives, investigates, and disseminates suspicious transaction reports (STRs). The unit includes a financial crime analyst as well as officers from Jersey's Police and Customs services. The JFCU received 1,034 STRs in 2006, and 1,162 in 2005. Approximately twenty-five percent of the STRs filed in 2005 and 2006 resulted in further police investigations.

The FIU, in conjunction with the Attorney General's Office, can trace, seize and freeze assets. It can obtain a confiscation order with a proven link to a crime. If the criminal has benefited from a crime, legitimate assets may be forfeited to meet a confiscation order. There is no maximum interval between the freezing of assets and when the assets are released. The Attorney General's Office may apply to the Court to confiscate assets previously frozen. Seized and forfeited proceeds from drug trafficking are placed in a separate fund which is then used to assist law enforcement in the fight against drug trafficking and to support harm reduction programs and education initiatives. Jersey allows limited civil forfeiture relating to cash proceeds of drug trafficking located at the ports and is considering introducing and implementing civil asset forfeiture powers.

Authorities in Jersey do not circulate the names of suspected terrorists and terrorist organizations listed on the United Nations Security Council Resolution (UNSCR) 1267 Sanctions Committee's consolidated list, nor do they circulate the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224, the EU designated list, or any other designated list. Institutions in the BOJ are expected to gather information of designated entities from the internet and other public sources. Jersey authorities have implemented sanction orders freezing accounts of individuals connected with terrorist activity.

Jersey's authorities have extensive license to cooperate with other domestic and international law enforcement and regulatory agencies. The JFSC cooperates with regulatory authorities to ensure that financial institutions meet anti-money laundering obligations. In 2005, the JFSC and the Jersey FIU worked together to deny the licensing of a Trust company and close a medium size business for failure to adhere to the AML legislation and guidance issued by the regulator. Internationally, the JFSC has reached agreements on information exchange with securities regulators in Germany, France, and the United States. The JFSC has a memorandum of understanding for information exchange with Belgium. The 1988 U.S.-UK Agreement Concerning the Investigation of Drug Trafficking Offenses and the Seizure and Forfeiture of Proceeds and Instrumentalities of Drug Trafficking, as amended in 1994, was extended to Jersey in 1996. Jersey shares forfeited assets with the U.S. pursuant to this agreement, and its laws enable Jersey to share assets in nondrug cases as well. Application of the 1988 UN Drug Convention was extended to Jersey on July 7, 1997. Jersey's FIU is a member of the Egmont Group.

The Bailiwick of Jersey has established an anti-money laundering program that in some instances exceeds international standards, and addresses its particular vulnerabilities to money laundering.

However, Jersey should establish reporting requirements for the cross-border transportation of currency and monetary instruments, and set penalties for violations. Jersey should also take steps to force its obligated entities to obtain verification documents for customers preceding the 1999 requirements. The BOJ should introduce civil asset forfeiture, and implement its new corruption law. Jersey should also ensure that supervisory authorities exist to apply standards and regulations to its port activity and "exempt companies" that are identical to those used in the rest of the jurisdiction. Jersey should take steps toward a more proactive role in fighting terrorism financing by circulating the UNSCR 1267 list as well as other lists, instead of relying on the entities to research names through online public sources. Jersey should continue to demonstrate its commitment to fighting financial crime by enhancing its anti-money laundering/counterterrorist financing regime in these areas of vulnerability.

Jordan

Despite significant growth in its financial services sector, Jordan is neither a regional nor offshore financial center, and is not considered a major venue for international criminal activity. The banking and financial sectors, including money service businesses, are supervised by competent authorities.

The Government of Jordan (GOJ) has yet to enact a comprehensive anti-money laundering law (AML). A draft law has been approved by the legal committee of the lower house of Parliament and there is hope that Parliament will pass the law during the 2006-2007 winter session. Currently, the Central Bank's suspicious transaction follow-up unit receives reports of suspicious financial activity from banks under the authority of Article 93 of the Banking Law of 2000, which obligates covered persons to notify the Central Bank of any transaction suspected of being related to any "crime or illegitimate act." In order to comply with international best practices, the Central Bank issued Instructions No. 29/2006 for banks in May 2006 which include important obligations concerning customer due diligence, politically exposed persons, wire transfers, record keeping, suspicious activity reporting, and internal policies and procedures, including the mandatory designation of a money laundering reporting officer. Instructions No.10/2001 impose similar, though less stringent, obligations on money service businesses. Article 52 of the Insurance Regulatory Act of 1999 criminalizes money laundering using insurance instruments. The Banking Law of 2000 (as amended in 2003) allows judges to waive banking secrecy provisions in any number of criminal cases, including suspected money laundering and terrorism financing.

In November 2006, Jordan's Parliament enacted an Anti-Terrorism law that prohibits the collection of funds with the intent that they be used in terrorist acts, and Article 147 of the Jordanian Penal Code prohibits banking transactions related to terrorist activity. However, Jordan does not yet have a statutory basis for the administrative freezing of the assets of designated terrorists listed on the UNSCR 1267 Sanctions Committee's consolidated list. Assets can be frozen and ultimately confiscated as part of a criminal investigation. 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.

Jordanian officials report that financial institutions file suspicious transaction reports and cooperate with prosecutors' requests for information related to narcotics trafficking and terrorism cases. There have not been any prosecutions or convictions for money laundering or terrorist finance. Legislation creating a Financial Intelligence Unit (FIU) is pending.

Charitable organizations are regulated by the Ministry of Social Development, and are governed by the Charitable Associations and Social Organizations Act of 1966. In accordance with this Act, organizations must register with the Ministry, which has the right to accept or reject the registration and conduct on-site inspections and review financial records. Furthermore, the Collection of Charitable Donations Regulation No. 1 of 1957 requires that all donations must be deposited in a bank

as soon as the collection process ends, and that the Ministry must be informed of the deposit. According to Central Bank Instructions No. 29/2006, banks must verify the identity of any charitable organization wishing to open an account. Moreover, the Penal Code stipulates that whoever collects donations, subscriptions, or contributions for an illicit organization shall be imprisoned for a period not to exceed six months.

There are six public free trade zones (FTZs) operating in Jordan, as well as 26 private FTZs. The FTZs operate under the supervision of the Free Zones Corporation as well as the Customs Department and are governed by the Free Zones Corporation Investment Regulation No. 43 of 1987 as well as the Customs Law. Both the Law and the Regulation prohibit the entrance of illegal material into the zones. The Customs Law grants the Minister of Finance the right to form joint committees comprised of staff from the Customs Department and the Free Zones Corporation to verify and inspect goods to ensure that no contraband is found in free zones. The Customs Law considers removal of goods from the free zones without the necessary customs clearances a smuggling offence. Currently, there is no cross border cash declaration requirement, although such a provision is contained in the draft AML law.

Jordan is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. Jordan has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Jordan is a charter member of the Middle East and North Africa Financial Action Task Force (MENAFATF) that was inaugurated in Bahrain in November 2004. In January 2007, Jordan assumes the presidency of this FATF-style regional body.

The Government of Jordan should enact a comprehensive anti-money laundering law that adheres to international standards including criminalizing money laundering from all serious crimes. The legislation should establish a Financial Intelligence Unit capable of sharing financial information with foreign counterparts. Jordan should develop a rigorous regime for the freezing, seizing and forfeiture of criminal assets and assets related to the financing of terrorism. The GOJ should become a party to the UN Convention against Transnational Organized Crime. Jordanian law enforcement and customs should examine forms of trade-based money laundering.

Kenya

Kenya does not have an effective legal regime to address money laundering. The Government of Kenya (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). As a regional financial and trade center for Eastern, Central, and Southern Africa, Kenya's economy has large formal and informal sectors. Many entities in Kenya are involved in exporting and importing goods, including a reported 800 registered international nongovernmental organizations (NGOs) managing approximately $1 billion annually. Annual remittances from expatriate Kenyans are estimated at $680 -780 million. Individual Kenyans and foreign residents also transfer money out of Kenya. 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.

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. Kenya has a large informal sector and a thriving network of cash-based, unrecorded transfers, primarily used by expatriates to send and receive remittances internationally. The large Somali refugee population in Kenya uses a hawala system to send and receive remittances; however, the GOK has no means to monitor hawala transfers.

Section 49 of the Narcotic Drugs and Psychotropic Substance Control Act of 1994 criminalizes money laundering related to narcotics trafficking and makes it punishable by a maximum prison sentence of

14 years. However, no cases of the laundering of funds from narcotics trafficking have ever been successfully prosecuted. The Act, together with Legal Notice No. 4 of 2001, the Central Bank of Kenya (CBK) Guidelines on Prevention of Money Laundering and enabling provisions of other laws, make money laundering a criminal offense but do not create an effective anti-money laundering (AML) regime.

In November 2006, the GOK published a proposed Proceeds of Crime and Anti-Money Laundering Bill. This bill is a revised version of a draft law introduced in 2004. It 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 both criminal and civil restraint, seizure and forfeiture. In addition, the proposed bill would authorize the establishment of an FIU and require 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 to be amended so that they will be consistent with the new bill when it is passed.

The new bill has some deficiencies. It does not mention terrorism, nor does it specifically define "offense" or "crime." The proposed legislation does not explicitly authorize the seizing 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 bill generated more support than the 2004 draft legislation, and senior GOK officials have claimed it is a high priority. However, the GOK did not table the bill in Parliament until November 22, and the bill lapsed when Parliament recessed on December 8. The bill will likely be tabled early in 2007.

The CBK is the regulatory and supervisory authority for Kenya's deposit-taking institutions and has responsibility for over 51 such entities, 95 foreign exchange bureaus, and mortgage companies and other financial institutions. Casinos are regulated by the Minister of Home Affairs, although its supervision of this sector is believed to be ineffective.

Forex bureaus were established and first licensed in January 1995 to foster competition in the foreign exchange market and to narrow the exchange rate spread in the market. As authorized dealers, forex bureaus conduct business and are regulated under the provisions of the Central Bank of Kenya Act (Cap 491). The CBK subsequently recognized that several bureaus were violating the Forex Bureau Guidelines, including dealing in third party checks and doing telegraphic transfers without the approval of the Central Bank. Those checks and transfers may have been used for fraud, tax evasion and money laundering. The CBK's Banking Supervision Department therefore issued Central Bank circular No. 1 of 2005 instructing all forex bureaus to cease immediately dealing in telegraphic transfers and third party checks. These new guidelines are issued under Section 33K of the Central Bank of Kenya Act, and took effect on January 1, 2007. They address third party checks and telegraphic transfers, and are also expected to enhance competition among bureaus.

In October 2000, the CBK issued regulations that 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 disclosure of financial information by the CBK to any monetary authority 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. There have been no arrests or prosecutions for money laundering or terrorist financing. Under the regulations, banks must maintain records of transactions over $100,000 and

international transfers over $50,000, and report them to the CBK. 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. Some commercial banks and foreign exchange bureaus do 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 law enforcement agency can demand information from any financial institution, if it has obtained a court order. However, 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. The contradiction highlights the need for "safe harbor" provisions and a robust anti-money laundering law.

Kenya has little in the way of cross-border currency controls. GOK regulations require that any amount of cash above $5,000 be disclosed at the point of entry or exit for record-keeping purposes only, but this provision is rarely enforced. The CBK guidelines call for currency exchange bureaus to furnish reports on a daily basis on any single foreign exchange transaction above $10,000, and on cumulative daily foreign exchange inflows and outflows above $100,000. Under September 2002 guidelines, foreign exchange dealers are required to ensure that cross-border payments are not connected with illegal financial transactions.

Kenya's vulnerability to money laundering was recently demonstrated by investigations revealing that 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. 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, indicate strongly that bank officials were complicit in these suspicious 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 transfers of funds to the United States and the United Kingdom were done in increments just below reporting thresholds of the receiving banks for large currency transactions, indicating a clear understanding of anti-money laundering controls.

The CBK Governor recommended in October 2006 that the Ministry of Finance revoke Charterhouse Bank's license so that CBK could liquidate the bank and compensate the innocent account holders. Charterhouse management and depositors filed numerous lawsuits to remove the statutory manager and reopen the bank. 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.) Charterhouse's owners are expected to mount a legal challenge to the bank's closure.

The Charterhouse Bank investigations revealed 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 been marketed through the normal wholesale and retail sectors. This case indicates that criminals have been taking advantage of Kenya's inadequate anti-money laundering regime for years by evading oversight and/or by 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 $100 million each year. However, in 2006 there was 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 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 redrafted the Anti-Terrorism Bill in 2006 to revise the rejected texts, but Muslim and human rights groups remain convinced the government could use it to commit human rights violations. The draft bill contains provisions that would strengthen the GOK's ability to combat terrorism; however, the GOK has yet to publish the bill or submit it to Parliament.

The CBK does not circulate the list of individuals and entities that have been included 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, it uses its bank inspection process to search for names on the OFAC list of designated people/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.

All charitable and nonprofit organizations are required 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, such penalties are rarely imposed. The government 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 it is suspected that charities and other nonprofit organizations handling millions of dollars are filing inaccurate or no annual reports. The Bureau plans to strengthen its capacity to review NGO registrations and annual reports for suspicious activities in 2007.

Drug trafficking-related asset seizure/forfeiture laws and their enforcement are weak and disjointed. Some underlying money laundering activities are criminalized under various Acts of Parliament. Apart from the seizure of intercepted drugs and narcotics, seizures of assets are rare. At present, the government entities responsible for tracing and seizing assets include the Central Bank of Kenya Banking Fraud Investigation Unit, the Kenya Police (through the Anti-Narcotics Unit and the Anti-Terrorism Police Unit), the Kenya Revenue Authority (KRA), and the Kenya Anti-Corruption Commission (KACC). Police must obtain a court warrant to demand bank account records or to seize an account. The police must present evidence linking the deposits to a criminal violation. 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. Although the KACC Director claimed that KACC had obtained court warrants to seize billions of shillings in 78 bank accounts belonging to corrupt politicians, businessmen and former senior civil servants in September 2006, no action was taken. 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. In the 2006 Transparency International Corruption Perceptions Index, Kenya is ranked 144 out of 163 countries measured. In 2004, Kenya acceded to the UN Convention against Transnational Organized Crime. Kenya is an active 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 regarding narcotics, terrorism financing, and other serious crime investigations. Kenya has cooperated with the United States and the United Kingdom, but lacks the institutional capacity, investigative skills, and equipment to conduct complex investigations independently.

Kenya is developing into a major money laundering country. The Government of Kenya should pass the proposed Proceeds of Crime and Anti-Money Laundering bill that includes the creation of a FIU. The Central Bank, law enforcement agencies, and the Ministry of Finance should work together more closely 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 and customs authorities should be trained to recognize and investigate trade-based money laundering methodologies and informal value transfer systems. Kenya should criminalize the financing of terrorism. Kenya should pass a law specifically authorizing the seizure of the financial assets of terrorists. Kenyan authorities should take steps to ensure that NGOs and suspect charities and nonprofit organizations follow international recognized norms regarding transparency and file complete and accurate annual reports.

Korea, Democratic Peoples Republic of

This is a reprint of last year's report as we have received no new information for 2006.

For decades, citizens of the Democratic Peoples Republic of Korea (DPRK) have been apprehended trafficking in narcotics and engaged in other forms of criminal behavior, including passing counterfeit U.S. currency and trade in counterfeit products, such as cigarettes.

Substantial evidence exists that North Korean governmental entities and officials have laundered the proceeds of narcotics trafficking and have been engaged in counterfeit and other illegal activities through a network of front companies that use financial institutions in Macau for their operations. On September 20, the U.S. Department of Treasury designated Banco Delta Asia SARL in Macau as a "primary money laundering concern" under Section 311 of the USA PATRIOT Act. The Department of the Treasury noted that the bank "…has been a willing pawn for the North Korean Government to engage in corrupt financial activities through Macau." The Federal Register Notice designating the bank cited "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, a significant number of which involved the arrest or detention of North Korean diplomats or officials.

In addition, indictments in the United States and the work of several corporate investigative teams employed by the holders of major United States and foreign cigarette and pharmaceutical trademarks have provided further compelling evidence of DPRK involvement in a wide range of criminal activities carried out in league with criminal organizations around the world, including trafficking in counterfeit branded items (cigarettes, Viagra), and high-quality counterfeit U.S. currency ("supernotes").

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, although these are gradually being phased out by 2009. Most money laundering appears to be associated with domestic criminal activity

or corruption and official bribery. Still, criminal groups based in South Korea maintain international associations with others involved in human and 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. 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 2006, also to the Korean police.

In 2006, the government implemented several measures to further strengthen its anti-money laundering regime by introducing mandatory currency transaction reporting (CTRs) for high-value cash transactions, on top of continued suspicious transaction reporting. Beginning in January 2006, financial institutions have been required to report within 24 hours all cash transactions of 50 million won ($49,213) or more by individuals to KoFIU. That reporting threshold will be lowered to 30 million won ($29,528) in 2008 and to 20 million won ($19,685) in 2010. Since January 2006, financial institutions have also been required to perform enhanced customer due diligence (CDD), thereby strengthening customer identification requirements set out in the Real Name Financial Transaction and Guarantee of Secrecy Act. Under the enhanced CDD 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 ($19,685) 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 (from $49,213 to $19,685). Improper disclosure of financial reports is punishable by up to five years imprisonment and a fine of up to 30 million won ($29, 528). Between January 1, 2002, and June 30, 2006, KoFIU received a total of 30,544 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, and 13,459 in 2005. In the first half of 2006, there were 10,386 STRs submitted to KoFIU, a 10 percent increase over the same period in 2005. Since 2002 through the first half of 2006, KoFIU has analyzed 29,626 of these reports and provided 4,268 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 4,268 cases referred to law enforcement agencies, investigations have been completed in 1,643 cases, with nearly half of those (806 cases) resulting in indictments and prosecution 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 2006, KoFIU continued to strengthen advanced anti-money laundering measures (such as the STR and CTR systems) to meet global standards such as Clause 5.8 of the Methodology for Assessing Compliance with the Financial Action Task Force (FATF) 40 Recommendations. KoFIU encouraged financial institutions including small-scale credit unions and cooperatives to adopt a differentiated risk-based

CDD 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 ($8.17 million) to be used to bribe politicians and bureaucrats, KoFIU in 2006 began considering revisions to the Financial Transaction Reports Act to impose anti-money laundering obligations on casinos. Intermediaries such as lawyers, accountants, or broker/dealers are not covered by Korea's money laundering controls. Any traveler carrying more than $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 terrorism financing. As of late 2006, two versions of a new counterterrorism bill are pending in Korea's unicameral legislature, the National Assembly. Previous attempts to pass similar bills 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. The proposed legislation is crafted to allow the Korean Government additional latitude in fighting terrorism, though general financial crimes and money laundering have already been criminalized in previously enacted laws. The pending counterterrorism bill, if passed, would 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. At this time, there are no known charitable or nonprofit entities operating in Korea that are used as conduits for the financing of terrorism.

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 at this time. Korean

banks have not identified any terrorist assets. There have been no cases of terrorism financing identified since January 1, 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 2006 Korea Customs Service report, 1,159 hawala cases worth 5. 26 trillion won ($4.2 billion) were recorded in 2002; 1,311 cases amounting to 2.2 trillion won ($1.84 billion) in 2003; 1,917 cases totaling 3.66 trillion ($3.2 billion) in 2004, and 1,901 cases worth 3.56 trillion won ($3.47 billion) in 2005. The majority of early hawala cases were related to the U.S. through 2004, but in 2005 the bulk of cases involved Japan (45 percent or $1.56 billion), followed by the U.S. (25 percent or $867 million) and the PRC (19 percent or $674 million).

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 2006, there were 371 reported cases of counterfeit dollars worth $36,450, compared to 1060 cases of $105,440 worth in the first nine months of 2005. Bank experts confirm that the amount of forged U.S. currency is on a sharp decline, reflecting local bank findings that the number of counterfeit $100 notes found during the first nine months of 2006 - about $36,100-fell to about one third of that found in the same period of 2005. In April 2005, the local press reported that police arrested a Korean who had smuggled $140,000 in $100 "supernotes" from China-a record amount for South Korea. However, no similar incidents were reported as of late 2006.

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. As of November 2006, Korea had seven FEZs, as a result of the June 2004 recategorization of the three port cities of Busan, Incheon, and Kwangyang as FEZs. They were recategorized from their previous designation of "customs-free areas" in order 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), and in 2004 hosted the APG annual

meeting. Korea also became a member of the Egmont Group in 2002. In August, 2006, the FATF invited Korea to become an Observer to the organization- the first step in gaining full membership. 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 31 countries/jurisdictions-the latest being Hong Kong-in November 2006.

The Government of the Republic of Korea should criminalize the financing and support of terrorism and should continue to move forward to adopt and implement its pending legislation. Among other priorities, the government should extend its anti-money laundering regime to nonfinancial institutions such as casinos and informal lending mechanisms widely recognized as potential blind spots. Just as importantly, 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. 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. The potential for the financing of terrorism through the misuse of charities continues to be a concern.

Kuwait has ten private local commercial banks, including two Islamic banks, all of which provide traditional banking services comparable to Western-style commercial banks. Kuwait also has two specialized banks, the Kuwait Real Estate Bank (KREB), which is in the process of converting to an Islamic bank, and the government-owned Industrial Bank of Kuwait. Both of these banks provide medium and long-term financing. With the conversion of KREB, there will be three Islamic banks, including the Kuwait Finance House (KFH) and Boubyan Islamic Bank.

The Kuwaiti banking sector opened to foreign competition under the 2001 Direct Foreign Investment Law, and the Central Bank of Kuwait (CB) has already granted licenses to four foreign banks: BNP Paribas, HSBC, Citibank, and the National Bank of Abu Dhabi; at present, the National Bank of Abu Dhabi has a license but no office in Kuwait. However, while foreign banks may now operate in Kuwait, they are only allowed to open one branch.

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 specifically cite terrorist financing as a crime. The law stipulates that banks and financial institutions may not keep or open anonymous accounts or accounts in fictitious or symbolic names, and that banks must require proper identification of both regular and occasional clients. The law also requires banks to keep all records of transactions and customer identification information for a minimum of five years, conduct anti-money laundering and terrorist financing training to all levels of employees, and establish proper internal control systems.

Law No. 35 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 CB 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 to the customs authorities, upon entering the country, of any national or foreign currency, gold bullion, or other precious materials in their possession valued in excess of 3,000 Kuwaiti dinars (approximately $10,000). 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 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 CB.

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 implement fully its current anti-money laundering law due in part to structural inconsistencies within the law itself. Kuwait's Financial Intelligence Unit is not an independent body in accordance with the current international standards, but rather is under the direct supervision of the Central Bank of Kuwait. In addition, vague delineations of the roles and responsibilities of the government entities involved continue to hinder the overall effectiveness of Kuwait's anti-money laundering regime. Cognizant of these shortcomings, the National Committee is currently drafting a revision of Law No. 35 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 CB instructions No. (2/sb/92/2002), which took effect on December 1, 2002, superseding instructions No. (2/sb/50/97). The revised instructions provide for, *inter alia*, customer identification and the prohibition of anonymous or fictitious accounts (Articles 1-5); the requirement to keep records of all banking transactions for five years (Article 7); electronic transactions (Article 8); the requirement to investigate transactions that are unusually large or have no apparent economic or lawful purpose (Article 10); the requirement to establish internal controls and policies to combat money laundering and terrorism finance, including the establishment of internal units to oversee compliance with relevant regulations (Article 14 and 15); and the requirement to report to the CB all

cash transactions in excess of $10,000 (Article 20). In addition, the CB distributed detailed instructions and guidelines to help bank employees identify suspicious transactions. At the Central Bank's instructions, banks are no longer required to block assets for 48 hours on suspected accounts in an effort to avoid "tipping off" suspected accountholders. The 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 UN 1267 Sanctions Committee's consolidated list. Financial entities are instructed to freeze any such assets immediately and for an indefinite period of time, pending further instructions from the Central Bank, which in turn receives its designation guidance from the MFA.

On June 23, 2003, the CB issued Resolution No. 1/191/2003, establishing the Kuwaiti Financial Inquiries Unit as an independent financial intelligence unit (FIU) within the Central Bank. The FIU is comprised of seven part-time CB officials and headed by the Central Bank Governor. The responsibilities of the FIU are to receive and analyze reports of suspected money laundering activities from the OPP, establish a database of suspicious transactions, conduct anti-money laundering training, and carry out domestic and international exchanges of information in cooperation with the OPP. Although the FIU should act as the country's financial intelligence unit, 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 an MOU 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. Reportedly, Kuwaiti officials agree that the current limits on information sharing by the FIU will have to be addressed by amending the law, which is currently under revision by the National Committee.

There are about 130 money exchange businesses (MEBs) operating in Kuwait that are authorized to exchange foreign currency only. None of these MEBs are formal financial institutions, and therefore are under the supervision of the Ministry of Commerce and Industry (MOCI) rather than the Central Bank. The CB has reached an agreement that tasks the MOCI with the enforcement of all anti-money laundering (AML) laws and regulations in supervising such businesses. Furthermore, MOCI will work diligently to encourage MEBs to apply for and obtain company licenses, and to register with the CB.

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 that are found to be in violation of the provisions of Law No. 35/2002 receive an official warning from MOCI for the first offense. The second and third violations result in closure for two weeks and one month respectively. The fourth violation results in revocation of the license and closure of the business. Reportedly, three exchange houses were closed in 2005: one for operating without a license, and the other two for violating MOCI's instructions.

In August 2002, the Kuwaiti Ministry of Social Affairs and Labor (MOSAL) issued a ministerial decree creating the Department of Charitable Organizations (DCO). The primary responsibilities of the new department are to receive applications for registration from charitable organizations, monitor their operations, and establish a new accounting system to insure that such organizations comply with the law both at home and abroad. The DCO has established guidelines for charities explaining donation collection procedures and regulating financial activities. The DCO is also charged with conducting periodic inspections to ensure that charities maintain administrative, accounting, and organizational standards according to Kuwaiti law. The DCO mandates the certification of charities' financial activities by external auditors, and limits the ability to transfer funds abroad only to select charities approved by MOSAL. 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 CB, which maintains a monthly database of all transactions conducted by charities. Unauthorized public donations, including Zakat (alms) collections in mosques, are also prohibited.

In 2005, the 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 in 2006, and plans are underway to 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). In November 2004, Kuwait signed the memorandum of understanding governing the establishment of the Middle East and North Africa Financial Action Task Force (MENAFATF), a FATF-style regional body. 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. In December 2005, the CB hosted a training seminar for mutual evaluation assessors of MENAFATF members.

Kuwait is a party to the 1988 UN Drug Convention. In May 2006, Kuwait ratified the UN Convention against Transnational Organized Crime. It 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; develop an independent Financial Intelligence Unit that meets international standards including the sharing of information with foreign FIUs; and improve international information sharing, as well as sharing between the government and financial institutions. 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. Rather, Kuwaiti law enforcement and customs authorities should be more active in identifying suspect behavior that could be indicative of money laundering, such as underground financial systems. Kuwait should become a party to both the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of the Financing of Terrorism.

Laos

Laos is on the fringe of mainland Southeast Asia's banking network. Laos is neither an important regional financial center, nor an offshore financial center, nor is it considered significant in terms of money laundering However, illegal timber sales, corruption, cross-border smuggling of goods, and illicit proceeds from the methamphetamine (ATS) known

locally as "ya ba" (crazy medicine), and domestic crime are sources of laundered funds. The Lao banking sector is dominated by state-owned commercial banks in need of extensive reform. 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 a small, low-tech environment. Reportedly, there is no notable increase in financial crime. While there is smuggling of consumer goods across the Mekong, this is not generally associated with money laundering. Rather, it is an easy way to avoid paying custom's duties and the inconvenience of driving across the bridge between Vientiane and Thailand. A special economic zone exists in the south. It is not considered particularly successful and there is no indication it is currently used to launder money or finance terrorism.

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. In March of 2006, the Prime Minister's Office issued a detailed decree 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. 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 current Financial Intelligence Unit, a committee located within the Bank of Laos, was established in 2004 and supervises financial institutions for their compliance with anti-money laundering/counter terrorist financing decrees and regulations. The Bank of Laos expects that this committee will be replaced by an operational unit with dedicated staff by early 2007. The FIU has no criminal investigative responsibilities, and is currently working with partner commercial banks to develop a standardized suspicious transaction report (STR). The bank estimates STRs will begin in 2007. There were none in 2006, nor were there any arrests for terrorist financing or money laundering. 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 $10,000-$50,000,), prison sentences from 10 to 20 years, and includes the death penalty. The Bank of Laos has circulated lists of individuals and entities on the UN 1267 sanction's coordinated list.

Lao law prohibits the export of the national currency, the Kip. 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 $2000. Cash must be declared when brought into the country and when departing. Failure to show declaration of incoming cash when exporting could lead to seizure

of the money or a fine. 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 Lao continue to build a framework of law and institutions; however, at this stage of development, enforcement of enacted legislation and decrees is weak.

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 money laundering.

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 also has observer status in the Asia Pacific Anti-Money Laundering Group, and plans to join in 2007. In order to comport with international standards, the Government of Laos should enact comprehensive anti-money laundering legislation, as decrees are not recognized by international organizations as the force of law. Laos should become a party to the UN 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. Casinos provide another source of laundered money. A significant amount of the proceeds of tax evasion are believed to originate from outside of Latvia. A portion of domestically-obtained criminal proceeds is thought to be derived 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. Although 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, there are ties between U.S.-derived drug money and the Latvian financial sector, and criminals have reportedly set up shell companies to launder drug money though the country.

Latvia currently is not considered to be an offshore financial center. Four special economic zones exist in Latvia providing a variety of significant tax incentives for the manufacturing, outsourcing, logistics centers, and trans-shipment 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 Financial and Capital Market Commission 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 anti-money laundering (AML) law, the Law on the Prevention of Laundering of Proceeds Derived from Criminal Activity, requires all institutions engaging in financial transactions to report suspicious activity to the financial intelligence unit (FIU). The legislation institutes customer

identification and record keeping requirements, as well as mandates the reporting of large cash transactions to the FIU. On February 1, 2004, Latvia adopted amendments to the AML law that expand the scope of reporting institutions to include auditors, lawyers, and high-value dealers, as well as credit institutions. The law lists four categories of entities obligated to report suspicious activities: participants in financial and capital markets (credit institutions, insurance companies, private pension funds, stock exchanges, brokerage companies, investment companies, credit unions, and investment consultants); organizers and holders of lotteries and gambling enterprises; companies engaged in foreign currency exchange; and individuals and companies who perform professional activities and services associated with financial transactions (money transfer services, tax consultants, auditors, auditing companies, notaries, attorneys, real estate companies, art dealers, and commodities traders). Another 2004 amendment provides for the inclusion of all offenses listed in the criminal law, including terrorism, as predicate offenses for money laundering. The amendments also provide the FIU with authority to block transactions for 45 days.

In addition to suspicious transactions, the law also mandates institutions to report unusual transactions to the FIU. Financial institutions receive a list of indicators that, when present, activate the reporting requirement for a financial institution. Many of the indicators are similar to those used to ascertain suspicious activities, and financial institutions are reportedly often uncertain which report is required to be filed. Most financial institutions rely on the list of indicators rather than evaluating transactions for suspicious activity. There is also a currency reporting requirement: obligated entities must report cash transactions, whether one large or several smaller, if the amount is equal to or exceeds 40,000 lats (approximately $73,000). Reporting is also required if, due to indicators that suggest unusual transactions, there is cause for suspicion regarding laundering or attempted laundering of the proceeds from crime. Financial institutions must keep transaction and identification data for at least five years after ending a business relationship with a client. If money laundering or terrorist financing is suspected, financial institutions have the ability to freeze accounts. 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.

In January 2005, the Council of Ministers adopted Regulation 55 that created a Council for the Prevention of Laundering of Proceeds Derived from Criminal Activity, a state-level AML body chaired by the Prime Minister. In April 2005, Latvia criminalized the misrepresentation of the beneficial owner. In May 2005, additional amendments to the AML and the criminal law were adopted that significantly enhanced the ability of Latvian law enforcement agencies to share information with one another and with Latvia's banking regulator, the Financial and Capital Markets Commission (FCMC). In 2005, Latvia also passed a new Criminal Procedures Law, which removed many procedural hurdles that had served as obstacles to law enforcement agencies when they attempted to aggressively investigate and prosecute 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.

In November 2005, Latvia passed legislation instituting a cross-border currency declaration requirement, which took effect on July 1, 2006. The law stipulates that all persons transporting more than 10,000 euros (approximately $12,787) in cash or monetary instruments into or out of Latvia, with the exception of into or out of other European Union member states, is obligated to declare the money to a customs officer, or, where there is no customs checkpoint, to a Border Guard. Because Latvia is part of the customs territory of the EU, people moving within the EU are not required to declare. Completing a declaration is mandatory for all who are transferring between Latvia and territory outside of the EU who have the requisite amount of cash or monetary instruments. Declarations are shared between Latvian government agencies.

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 additional information on incorporation and registration. In June 2005, the GOL increased sanctions against banks for noncompliance, providing for fines up to $176,000. Latvia does not have secrecy laws that prevent the disclosure of client and ownership information to bank supervisors or law enforcement officers. Reporting individuals are protected by safe harbor provisions in the law.

Since July 2001, the Finance and Capital Market Commission (FCMC) has served as the GOL's unified public financial services regulator, overseeing commercial banks and nonbank financial institutions, the Riga Stock Exchange, and insurance companies. The Bank of Latvia supervises the currency exchange sector. The FCMC conducts regular audits of credit institutions and applies sanctions to companies that fail to file mandatory reports of unusual transactions. The FIU also works to ensure accurate reporting by determining if it has received corresponding STRs when suspicious transactions occur between Latvian banks.

The FCMC has distributed regulations for customer identification and detecting unusual and suspicious transactions, as well as regulations regarding internal control mechanisms that financial institutions should have in place. The May 2005 amendments to the AML law gave the FCMC the authority to share information with Latvian law enforcement agencies and receive data on potential financial crime patterns uncovered by police or prosecutors. The June 2005 amendments to the Criminal Procedures Law added an article criminalizing the deliberate provision of false information about a beneficiary to a credit or a financial institution.

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. In May 2004, the ALCB adopted the regulations on the Prevention of Money Laundering as guidance. Under the leadership of the ALCB and at the urging of the FCMC, Latvian banks collectively reviewed existing customer relationships in the first half of 2005, which resulted in the closure of more than 100,000 accounts connected to customers unwilling or unable to comply with the enhanced due diligence requirements. In June 2005, the ALCB adopted a Declaration on Taking Aggressive Action against Money Laundering, which was signed by all Latvian banks. In 2005, the ACLB also adopted a voluntary measure, which all of the banks observed, to limit cash withdrawals from automated teller machines to 1,000 lats (approximately $1,834) per day. Member banks respect the ACLB guidelines. In addition to acting as an industry representative to government and the regulator, the ACLB organizes regular education courses on anti-money laundering/ counter terrorism financing (AML/CTF) issues for bank employees.

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 the overall responsibility for coordination, application and assessment of Latvia's AML policy and its effectiveness. During 2006, the Control Service received more than 27,000 reports of suspicious and unusual transactions. The Control Service received 26,302 reports in 2005 and 16,479 reports in 2004. Approximately 53 percent of the reports received in 2005 and 2006 were for suspicious transactions and 47 percent were classified as unusual transactions.

The Control Service conducts a preliminary investigation of the suspicious and unusual reports and then may 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 State Police; the Economic 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, ACB) for crimes committed by public officials; the Security Police (for cases concerning terrorism and terrorism financing); and other law enforcement authorities.

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

The Prosecutor General's Office maintains a staff of seven prosecutors to prosecute cases linked to money laundering. The individuals comprising the staff have been subjected to a special clearance process. In the first eight months of 2006, the Prosecutor General's Office received nine new money laundering cases for prosecution; of these, it referred six cases to court for the criminal offense of money laundering. Three individuals received convictions, and sentences including time in jail, in two cases.

The adoption of Latvia's new Criminal Procedures Law in 2005 provided additional measures for the seizure and forfeiture of assets. The law allows law enforcement authorities to better identify, trace, and confiscate criminal proceeds. Investigators have the ability to initiate an action for the seizure of assets recovered during a criminal investigation concurrently with the investigation itself (previously this was possible only when the investigation was complete).

In 2006, the Latvian FIU issued 125 orders to freeze assets, freezing a total of 12,645,000 Lats (approximately $23.5 million). Proceeds from any seizures or forfeitures pass to the State budget. Latvia's FIU reports that cooperation from the banking community to trace and freeze assets has been excellent.

The GOL has initiated a number of measures aimed at combating the financing of terrorism. It has issued regulations to implement the sanctions imposed by United Nations Security Council Resolution (UNSCR) 1267. The regulations require that financial institutions report to the Control Service transactions related to any suspected terrorists or terrorist organizations 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 sends 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. Freezing of terrorist assets falls under the same mechanism as with other crimes, but includes involvement by the Latvian Security Police. Any associated investigations, asset or property seizures, and forfeitures are handled in accordance with the new Criminal Procedures Law. On June 1, 2005, Latvia amended its Criminal Law supplementing it with a new Article 88-1 that specifically criminalizes the financing of terrorism, meeting the requirements of UNSCR 1373.

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. Reportedly, there are some concerns regarding the willingness of the banking sector to comply with the government, as evidenced by the banking sector's response to the 2005 action. The United States issued a final rule imposing a special measure against only one of the two banks, VEF Banka, as a financial institution of primary money laundering concern, on August 14, 2006.

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

Latvia is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). Latvia underwent a joint International Monetary Fund (IMF)/MONEYVAL evaluation in March 2006 which assessed the country's AML regulatory and legal framework. This assessment was approved as MONEYVAL's third-round evaluation of Latvia in September 2006. The Control Service is a member of the Egmont Group and has agreements on information exchange with sixteen counterpart FIUs.

Latvia is a party to the UN International Convention for the Suppression of the Financing of Terrorism and eleven other multilateral counterterrorism conventions. Latvia is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN Convention against Corruption. A Mutual Legal Assistance Treaty (MLAT) has been in force between the United States and Latvia since 1999.

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 AML law and Criminal Procedures Law, taking steps to increase information sharing and cooperation between law enforcement agencies at the working level. The GOL should lower the threshold for the reporting of currency transactions. The GOL should also strengthen its ability to aggressively prosecute and convict those involved in financial crimes. Latvian authorities should also clarify the distinction between unusual transaction reports and suspicious transaction reports in its guidance to the obliged entities.

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 September 2006, there were 63 banks (54 commercial banks and nine investment banks) operating in Lebanon with total deposits of $59.7 billion. Four U.S. banks and bank representative offices operate in Lebanon: Citibank, American Express Bank, the Bank of New York, and JP Morgan Chase Bank.

The Central Bank (Banque du Liban) (CBL) regulates all financial institutions and money exchange houses. Banking sources emphasize their belief that Lebanon is not a significant financial center for money laundering, but acknowledge that it does have a number of vulnerabilities. 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 $3.5-4 billion yearly.

Laundered criminal proceeds come primarily from domestic criminal activity. Money laundering proceeds are largely controlled by organized crime. During 2006, the banking sector has seen two cases of bank fraud consisting of embezzlement by bank employees in branch offices and one case of fraud by a money dealer. 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 is not permitted in Lebanon, nor are offshore trusts or offshore insurance companies. Legislative Decree No. 46, dated June 1983, governs offshore companies. It restricts offshore companies' activity to negotiating and signing agreements 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 Registry, and the owners of an offshore company must submit a copy of their identification. Moreover, the Registrar of the Beirut Court keeps a special register, in which all

information about the offshore company is retained. A draft law amending legislation on offshore companies to make it WTO compliant was still pending in Parliament as of early November 2006.

There are currently two free trade zones operating in Lebanon, at the Port of Beirut and at the Port of 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. If Customs suspects trade-based money laundering or terrorism finance, it reports it to Lebanon's financial intelligence unit (FIU), the Special Investigation Commission (SIC). 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 when large amounts of cash are found.

In 2004, Lebanon passed a law requiring diamond traders to seek proper certification of origin for imported diamonds; the Ministry of Economy and Trade is in charge of issuing certification for re-exported diamonds. This law was designed to prevent the traffic in conflict diamonds, and allowed Lebanon to join the Kimberley Process on September 20, 2005. In August 2003, Lebanon passed a decree prohibiting imports of rough diamonds from countries that are not members of the Kimberley Process. However, in 2005, investigations by Global Witness, a nongovernmental organization, discovered that according to Lebanese customs data, Lebanon imported rough diamonds worth $156 million from the Republic of Congo (ROC), a country removed from the Kimberley Process Certification Scheme for having a "massive discrepancy" between its actual diamond production and declared exports. This documented example of suspect imports from the ROC throw serious doubts on Lebanon's commitment to counter the trade in conflict diamonds. Moreover, there have been consistent reports that many Lebanese diamond brokers in Africa are engaged in the laundering of diamonds—the most condensed form of physical wealth in the world.

Lebanon has a large expatriate community that is found 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. Reportedly, many 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. There are also reports that many in the Lebanese expatriate business community willingly or unwillingly give "charitable donations" to representatives of Hezbollah. The funds are then repatriated or laundered back to Lebanon.

Lebanon has continued to make progress toward developing an effective money laundering and terrorism finance regime by incorporating the Financial Action Task Force (FATF) Recommendations. In 2002, Lebanon was removed from the FATF's Non-Cooperative Countries and Territories list (NCCT), after 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 twenty 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 CBL regulates private couriers who transport currency. Western Union and Money Gram are licensed by the CBL 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 the CBL. Law No. 318 clarified the CBL'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 an FIU, called the Special Investigation Commission (SIC), which 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. In spring 2006, the SIC started work on a self-assessment in order to further enhance compliance with FATF Recommendations, and to prepare for a potential assessment by international bodies, expected in late 2007 or early 2008.

Since its inception, the SIC has been active in providing support to international criminal case referrals. From January through October 2006, the SIC investigated 118 cases involving allegations of money laundering and terrorist financing activities. Of these cases, five were originated at U.S. Government request. Two of the 118 cases were related to terrorist financing. Bank secrecy regulations were lifted in 56 instances. Ten cases were transmitted by the SIC to the general state prosecutor for further investigation. As of early November 2006, no cases were transmitted by the general state prosecutor to the penal judge. The general state prosecutor reported three cases to the SIC for the freezing of assets. One case involved individuals convicted of terrorism charges, another case involved individuals related to Iraq's former regime, and the third case involved individuals convicted of drug charges. From January to October 2006, the SIC froze the accounts of 17 individuals in five of the 118 cases investigated. Total dollar amounts frozen by the SIC in these five cases is about $1.4 million. The SIC has also worked with the UN International Independent Investigation's Commission (UNIIC) investigation into the assassination of Rafiq Hariri, helping the international inquiry lift bank secrecy laws on certain accounts and freeze the assets of suspects. As a result, dollar amounts frozen by the SIC amounted to $22 million in 2005.

During 2003, Lebanon adopted additional measures to strengthen efforts to combat money laundering and terrorism 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 the police, as well as with the office of the general state prosecutor. In 2005, a SIC Remote Access Communication (SRAC) system was put in place for the exchange of information between the SIC, Customs, the Internal Security Forces (ISF) anti-money laundering and terrorist finance 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 2006.

In order to more effectively combat money laundering and terrorist financing, Lebanon also adopted two important 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 (which distinguishes between "terrorism" and "resistance"). 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.

Lebanon was one of the founding members of the Middle East and North Africa Financial Action Task Force (MENAFATF), a FATF-style regional body that promotes best practices to combat money laundering and terrorist financing in the region. It was inaugurated on November 30, 2004, in Bahrain. As it assumed its presidency for the first year, Lebanon hosted the second MENAFATF plenary in September 2005. A third MENAFATF plenary was held in March 2006 in Cairo where, at Lebanon's initiative, the U.S.-MENA Private Sector Dialogue (PSD) was launched. Lebanon assumed the presidency of the U.S-MENA PSD for the first year.

Lebanon has endorsed the Basel Committee's "Core Principles for Effective Banking Supervision" and is compliant on 24 out of the 25 "Core Principles." Compliance with the pending "Core Principle" is being addressed, and a draft law providing legal protection to bank supervisors awaits cabinet approval. On October 31, 2006, the Banking Control Commission performed a self-assessment, to be completed before the end of January 2007. Banks are compliant with the Basel I Capital Accords and are preparing to comply with the three pillars of the Basel II recommendations. The CBL and the Banking Control Commission are issuing circulars to ensure the banking sector is compliant with Basel II recommendations by January 1, 2008.

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. The SIC as of early November 2006 had signed fifteen memoranda of understanding with other FIUs concerning international cooperation in anti-money laundering and combating terrorist financing. The SIC cooperates with competent U.S. authorities on exchanging records and information within the framework of Law 318.

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 Government of Lebanon continues to improve its efforts to develop an effective anti-money laundering and counterterrorism finance regime. 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. 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. It should become a party to the UN Convention against Corruption and the UN International Convention for the Suppression of Terrorist Financing. Per Financial Action Task Force Special Recommendation Nine, 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.

Libya

Libya is not considered to be an important financial sector in the Middle East and northern Africa. The Libyan economy depends primarily upon revenues from the oil sector, which contribute practically all export earnings and about one-quarter of GDP. Oil revenues and a small population give Libya one of the highest per capita GDPs in Africa, but little of this income flows down to the lower levels of society. Libya has a cash-based economy and large underground markets. Libya is a destination for smuggled goods, particularly alcohol and black market/counterfeit goods from sub-Saharan Africa and from Egypt. Contraband smuggling includes narcotics, particularly hashish/cannabis and heroin. Libya is not considered to be a production location for illegal drugs, although its geographic position, long borders and lax immigration policies make it a transit point. Libya is also a transit and destination country for human trafficking originating in sub-Saharan Africa and Asia. Many victims willingly migrate to Libya en route to Europe with the help of smugglers. Reportedly, human smuggling networks force some victims into prostitution or to work as laborers and beggars to pay off their smuggling debts. Profits are laundered. Hawala and informal value transfer networks are present.

The Libyan banking system consists of a Central Bank, six state-owned commercial banks, forty-eight national banks and a handful of privately-owned Libyan banks. Libyan banks suffer from a lack of modern equipment and trained personnel, and substantial investment in both will be required to bring Libyan banks up to international standards. Libyan banks offer little in the way of services for their customers, and most Libyans make little use of the banking system. The Libyan Banking Law No. 1 of 2005 allows for the entry of foreign banks into Libya although with difficult entry and operating terms and requirements that, combined with a history of Libyan government policy reversals, have precluded foreign bank entry to date. Libya is not considered to be an offshore financial center. Offshore banks, international business companies and other forms of exempt/shell companies are not licensed by the Libyan government.

Libya has shown some commitment to privatize its public banks. During the past year, the ongoing privatization of Sahara Bank has resulted in the sale of approximately 40 percent of its shares to individual investors The Central Bank continues to formulate a program of banking sector modernization and has hired western consulting firms to assist in reforms. Libya is also cooperating with both the IMF and World Bank by soliciting their advice and assistance for economic reforms. In general, training and resources are lacking for anti-money laundering awareness and countermeasure implementation. A considerable transition time is anticipated while Libya's banking system is reformed and gradually brought back into the international system following the lifting of UN and U.S. sanctions.

The Central Bank is responsible for the establishment of regulations relevant to combating money laundering and terrorist finance under the terms of Article 57 of Banking Law No. 1 of 2005. Money laundering is illegal in Libya, and terms and penalties are clearly laid out in Banking Law No. 2 of 2005 on Combating Money Laundering. This law does not make specific mention of drug-related money laundering. These crimes are dealt with under Libya's Penal Code, Criminal Procedures Law, and related supplementary laws. Penalties for money laundering under Law No. 2 include

imprisonment (for an unspecified duration) and a fine equal to the amount of relevant illegal goods/property. An increased penalty is used if the malefactor participated in the predicate offense, whether as a perpetrator or accomplice. Penalties ranging from 1,000 to 10,000 Libyan dinars (approximately $770 to $7,700) are also imposed on persons withholding information on money laundering offenses, persons warning offenders of an ongoing investigation and persons in violation of foreign currency importation regulations. The offense of falsely accusing others of money laundering offenses is punishable by imprisonment of no less than a year.

Banking Law No. 2 directs the Central Bank to establish a Financial Information Unit (FIU). It also establishes a National Committee for Combating Money Laundering to be chaired by the Governor or Deputy of the Central Bank. The National Committee will also include representatives from the Secretariat of the General People's Committee for Financial and Technical Supervision, the Secretariat of the General People's Committee for Justice, the Secretariat of the General People's Committee for Public Security, the Secretariat of the General People's Committee for Finance, the Secretariat of the General People's Committee for Economy and Trade, the Secretariat of the General People's Committee for Foreign Liaison and International Cooperation, the Customs Authority and the Tax Authority.

Libyan banks are required to record and report the identity of customers engaged in all transactions. Records of transactions are retained for a considerable (but indeterminate) period, although a lack of computerized records and systems, particularly among Libya's more than forty-eight regional banks and branches in remote areas of the country, negate reliable record-keeping and data retrieval.

Libya's Banking Law No.1 forbids "possessing, owning, using, exploiting, disposing of in any manner, transferring, transporting, depositing, or concealing illegal property in order to disguise its unlawful source." The broad scope of the law, and its complimentary relationship to existing criminal law, extends the scope of money laundering controls and penalties to nonbanking financial institutions. All entities, either financial or nonfinancial in nature, are required by law to report money laundering activity to Libyan authorities under penalty of law. The Central Bank is responsible for supervision of all banks, financial centers and money changing institutions. All banks are required to undergo an annual audit and establish an administrative unit called the "compliance unit" which is directly subordinate to the board of directors. The Central Bank's Banking Supervision Division is also responsible for examining banks to ensure that they are operating in compliance with law.

Libya established a Financial Information Unit (FIU) under the terms of Banking Law No. 2. The Central Bank is responsible for establishing and housing the Libyan FIU. The most recent reporting available indicates that the FIU is still in its formative stages, and individuals seconded by the Central Bank to the FIU require additional training in order to be fully effective.

The FIU is tasked to gather all reports on suspicious transactions from all financial and commercial establishments and individual persons. The FIU is authorized by law to exchange information and reports on cases suspected of being linked to money laundering activities with its counterparts in other countries, in accordance with Libya's international commitments. All banks operating in Libya are required by law to establish a "Subsidiary Unit for Information on Combating Money Laundering" responsible for monitoring all activities and transactions suspected of being linked to money laundering activities. The FIU is responsible for reporting this information to the Governor of the Central Bank for appropriate action. However, given the limitations of the Libyan banking sector both in terms of human and technological resources and the lead time necessary to establish new internal mechanisms, these subsidiary units are either non-existent or nonfunctional in most cases. All entities cooperating with the FIU and/or law enforcement entities are granted confidentiality. Furthermore, anyone reporting acts of money laundering before they are discovered by Libyan authorities is exempted from punishment under the law (safe harbor). There is no reliable information on the

number of suspicious transaction reports (STRs) issued in 2006, nor information on the scope of prosecutions and convictions on the part of Libyan government authorities.

It is illegal to transfer funds outside of Libya without the approval of the Central Bank. Cash courier operations are in clear violation of Libyan law. It is estimated that up to ten percent of foreign transfers are made through illegal means (i.e., not through the Central Bank). Libya is seeking foreign assistance to bring tighter control over these transactions. However, fund transfers by illegal immigrants (mainly from sub-Sahara Africa) are difficult for the Libyan government to monitor, particularly transfers by criminal organizations. It is estimated that there are currently up to two million illegal immigrants in Libya. It is illegal for these workers to take cash out of the country, however some do engage in smuggling and there are illicit transfers of goods and currency across Libya's long land borders.

Informal hawala money dealers (hawaladars) exist in Libya, and are often used to facilitate trade and small project finance. Libyan officials have indicated that they intend to require registration of all hawaladars in the near future. Many payments and transactions take place outside the banking system, often using cash, so as to avoid the scrutiny of the Libyan government. This is done largely for practical reasons, as Libya's socialist practices and commercial rivalries among regime insiders discourage disclosure of income and business transactions. Until the recent revision of the tax code, rates of up to 80-90 percent encouraged off-the-book transactions.

Reportedly, there is no evidence of extensive money laundering or terrorist financing taking place in the Free Trade Zone (FTZ) in the city of Misurata. Misurata, 210 kilometers east of Tripoli, is currently Libya's sole operating FTZ. Projects in the free zone enjoy standard "Five Freedoms" privileges, including tax and customs exemptions. At present, the zone occupies 430 hectares, including a portion of the Port of Misurata.

Libya is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. Libya is a party to all 12 of the UN Conventions and Protocols dealing with terrorism, including the International Convention for the Suppression of the Financing of Terrorism. However, Libya has not criminalized terrorist financing. Nor is there any indication that Libya has circulated UN or U.S. lists of terrorist entities or made any effort to freeze, seize or forfeit assets of suspected terrorists or financiers of terrorism.

In 2006, the Department of State rescinded Libya's designation as a State Sponsor of Terrorism. The Government of Libya (GOL) should enact counterterrorist financing legislation and adopt anti-money laundering and counterterrorist finance policies and programs that adhere to world standards. Joining the Middle East and North Africa Financial Action Task Force would assist Libya in that regard. Libya should continue to modernize its banking sector and adopt full transparency procedures. Tax reform should continue so as to shrink the underground economy. Working with the international community, the Libyan FIU and financial police should avail themselves of training. Appropriate entities should become familiar with money laundering and terrorist finance methodologies. In particular, Libyan law enforcement and customs authorities should examine the underground economy, including smuggling networks, and informal value transfer systems. The GOL should adopt measures that combat corruption in government and commerce. Government statistics on the number of money laundering investigations, prosecutions, and convictions should be made publicly available.

Liechtenstein

The Principality of Liechtenstein's well-developed offshore financial services sector, relatively low tax rates, liberal incorporation and corporate governance rules, and tradition of strict bank secrecy have contributed significantly to the ability of financial intermediaries in Liechtenstein to attract funds from abroad. These same factors have historically made the country attractive to money launderers and

tax evaders. Although the principality has made progress in its efforts against money laundering, accusations of misuse of Liechtenstein's banking and financial services sectors persist.

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 account for slightly less than 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 in order to further expand the list of predicate offenses. Article 165 criminalizes laundering one's own funds and imposes penalties for money laundering. However, negligent money laundering is not addressed.

The first general anti-money laundering legislation was added to Liechtenstein's laws in 1996. Although the 1996 law applied some money laundering controls to financial institutions and intermediaries operating in Liechtenstein, the anti-money laundering 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 anti-money laundering regime.

Liechtenstein's primary piece of anti-money laundering legislation, the Due Diligence Act (DDA) of November 26, 2004, entered into force on February 1, 2005. The act repealed a number of prior laws, including the 1996 Due Diligence Act and its amendments. The DDA applies to banks, e-money institutions, casinos, dealers in high-value goods, and a number of other classes of entities. Along with the January 2005 Due Diligence Ordinance, the DDA sets out the basic requirements of the anti-money laundering regime: customer identification, suspicious transaction reporting, and record keeping. The act mandates that banks and postal institutions not engage in business relationships with shell banks nor maintain passbooks, accounts, or deposits payable to the bearer. The legislative revision also focused on the inclusion of measures to combat terrorist financing. For instance, the DDA expanded the scope of STR (suspicious transaction reporting) to including terrorist financing.

The GOL announced that by 2008 it would implement a new set of EU regulations requiring that money transfers above 15,000 euro (approximately $17,680) be accompanied by information on the identity of the sender, including his or her name, address, and account number. The proposed measures will ensure that this information will be immediately available to appropriate law enforcement authorities and will assist them in detecting, investigating, and prosecuting terrorists and other criminals.

The Financial Market Authority (FMA) serves as Liechtenstein's central financial supervisory authority. Beginning operations on January 1, 2005, FMA 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. It oversees 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 STRs relating to money laundering and terrorist financing. The EFFI became operational in March 2001 and a member of the Egmont Group three months later. The EFFI has set up a database to analyze its STRs and has access to various governmental databases, although it cannot seek additional financial information

unrelated to a filed STR. 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 and based on a suspicion, rather than the previous standard of "a strong suspicion."

In 2005, the number of STRs decreased by 17.5 percent from the previous year to 193. Of these 193 reports, the majority were submitted by banks (54 percent) and professional trustees (38 percent). As in 2004, fraud and money laundering remained the most prevalent types of offenses indicated by the entities submitting STRs to the FIU. The share of STRs involving fraud decreased from 48 percent to 45 percent, while the share of STRs involving money laundering increased from 20 percent to 27 percent. There is no similar data available for 2006.

In 2005, the FIU forwarded 72 percent of the total number of STRs it received to prosecution authorities, compared with 79 percent in 2004 and 72 percent in 2003. In the reporting year, 22.3 percent of the beneficial owners indicated in STRs were German nationals, followed by Swiss and U.S. nationals with 14.5 percent each. Austrian, British, and Dutch citizens each accounted for 4.1 percent of beneficial owners indicated in STRs, and Liechtenstein nationals made up only 3 percent of beneficial owners mentioned. In terms of the location of the suspected predicate offense (as mentioned in STRs), Canada and the United States accounted for the most funds, with about $403 million (500 million Swiss francs) and $360 million (450 million Swiss francs) respectively.

In 2005, the EFFI received 89 inquiries from 13 foreign FIUs, 25 percent fewer than in 2004. In the same period, the EFFI submitted 103 inquiries to 18 different countries, down from 134 inquiries in 2004. The most frequent judicial cooperation requests originated from or were directed to the U.S., Germany, Switzerland, and Austria.

Liechtenstein has in place 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 legal assistance is granted on the basis of dual criminality—the offense must be a criminal offense in both jurisdictions. Article 235A provides for the sharing of confiscated assets, and this has been used in practice. Liechtenstein has not adopted the EU-driven policy of reversing the burden of proof by making it necessary for the defendant to prove that he had acquired assets legally (instead of the state having to prove he had acquired them illegally).

A series of amendments to Liechtenstein law, adopted by Parliament on May 15, 2003, include a new criminal offense for terrorist financing along with amendments to the Criminal Code and the Code of Criminal Procedure. Liechtenstein also has issued ordinances to implement United Nations Security Council Resolutions (UNSCRs) 1267 and 1333. Amendments to the ordinances in October and November 2001 allow the GOL to freeze the accounts of individuals and entities that were designated pursuant to these UNSCRs. The GOL updates these ordinances regularly.

The GOL has also 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 and was reaffirmed through an exchange of diplomatic notes on July 14, and October 27, 2006. 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 EFFI has in place memoranda of understanding (MOUs) with the FIUs in Belgium, Monaco, Croatia, Poland, Russia, Switzerland, and Georgia. Further MOUs are being prepared with France, Italy, Canada, Malta, and San Marino.

Liechtenstein is a member of the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). 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. Liechtenstein has also signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Liechtenstein has endorsed the Basel Committee's "Core Principles for Effective Banking Supervision" and has adopted the EU Convention on Combating Terrorism.

The Government of Liechtenstein has made progress in addressing shortcomings in its anti-money laundering regime. It should continue to build upon the foundation of its evolving anti-money laundering and counterterrorist financing regime. Liechtenstein should become a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. Per FATF Special Recommendation Nine, Liechtenstein should require reporting of cross-border currency movements. The data should be shared with EFFI, the financial intelligence unit. Authorities should ensure that trustees and other fiduciaries comply fully with all aspects of the new anti-money laundering legislation and attendant regulations, including the obligation to report suspicious transactions. The EFFI should be given 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. There appears to be an over-reliance on STRs to initiate money laundering and financial crimes investigations; Liechtenstein law enforcement entities should become more pro-active in this regard. The GOL should criminalize "negligent money laundering" and should publish the annual number of arrests, prosecutions, and convictions for money laundering.

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. Its strict bank secrecy laws allow international financial institutions to benefit from and operate a wide range of services and activities. With nearly $ 2.2 trillion in domiciled assets, Luxembourg is the second largest mutual fund investment center in the world, after the United States. Luxembourg is considered an offshore financial center, with foreign-owned banks (many of which enjoy ring-fenced tax benefits) accounting for a majority of the nation's total bank assets. 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. For this reason (and also due to the proximity of three of these nations to Luxembourg), a significant share of Luxembourg's suspicious transaction reports (STRs) are generated from transactions involving clients in these countries. While Luxembourg is not a major hub for illicit drug distribution, the size and sophistication of its financial sector create opportunities for money laundering, tax evasion, and other financial crimes.

As of September 2006, 154 banks, with a balance sheet total reaching 824 billion euros (approximately $1.05 trillion), were registered within Luxembourg. In addition, as of September 2006, a total of 2,158 "undertakings for collective investment" (UCIs), or mutual fund companies, whose net assets had reached over 1.7 trillion euros (approximately $2.18 trillion) by the end of September 2006, were operating out of Luxembourg. Luxembourg has about 15,000 holding companies, 95 insurance companies, and 260 reinsurance companies. As of January 2006, the Luxembourg Stock Exchange listed over 36,000 securities issued by nearly 4,100 entities from about 100 different countries. Legislation passed in June 2004 permits the registration of venture capital funds (Societe d'investissement en capital a risqué, or "SICAR"). As of September 2006, 82 SICARs had been registered.

Luxembourg's financial sector laws are modeled to a large extent on EU directives. The Law of July 7, 1989, updated in 1998 and 2004, serves as Luxembourg's primary anti-money laundering (AML) and terrorist financing law, criminalizing the laundering of proceeds for an extensive list of predicate

offenses, including narcotics trafficking. The Law of April 5, 1993 implements the EU's 1991 First Anti-Money Laundering Directive and includes among its provisions customer identification, record keeping, and suspicious transaction reporting requirements. The Act of August 1, 1998 expands the list of covered entities and adds corruption, weapons offenses, and organized crime to the list of predicate offenses for money laundering. The Act of June 10, 1999 further expands anti-money laundering provisions. On May 23, 2005, a new law was passed which added corruption in the private sector to the list of money laundering predicate offenses. Fraud committed against the European Union has also been added to the list of offenses. Although only natural persons are currently subject to the law, the government has been preparing a draft bill that would add legal persons to its jurisdiction.

In an effort to bring Luxembourg into full compliance with the requirements of the EU's Second Money Laundering Directive, on November 12, 2004, Parliament approved legislation updating the nation's anti-money laundering laws. These legislative amendments formally transferred the requirements of the EU's Second Money Laundering Directive into domestic law. In October 2005, the Commission de Surveillance du Secteur Financier (CSSF) distributed a circular to the financial industry publicizing the November 2004 law and offering advice on suggested best practices. The 2004 amendments also broaden the scope of institutions subject to money laundering regulations. Under the current law, banks, pension funds, insurance brokers, UCIs, management companies, external auditors, accountants, notaries, lawyers, casinos and gaming establishments, real estate agents, tax and economic advisors, domiciliary agents, insurance providers, and dealers in high-value goods, such as jewelry and cars, are now considered covered institutions. AML law does not cover SICAR entities.

All covered entities are required to file STRs with the financial intelligence unit (FIU) and, though not legally required, are expected to send copies of their reports to their respective oversight authorities. The banking community generally cooperates with enforcement efforts to trace funds and seize or freeze bank accounts; the track record of cooperation by notaries and others is still being tested, given the legislation has only been in effect for the past year. Financial institutions are required to retain pertinent records for a minimum of five years; additional commercial rules require that certain bank records be kept for up to ten years. The AML law also contains "safe harbor" provisions that protect obliged individuals and entities from legal liability when filing STRs or assisting government officials during the course of a money laundering investigation. The 2004 amendments also contain new requirements regarding financial institutions' internal AML programs. They impose strict "know your customer" requirements, mandating their application to all new and existing customers, including beneficial owners, trading in goods worth at least 15,000 euros. If the transaction or business relationship is remotely based, the law details measures required for customer identification. Financial institutions must ensure adequate internal organization and employee training, and must also cooperate with authorities, proactively monitoring their customers for potential risk. "Tipping off" has also been prohibited.

Under Luxembourg law the secrecy rules are waived in the prosecution of money laundering and other criminal cases. No court order is required to investigate otherwise secret account information in suspected money laundering cases or when a STR is filed. Financial professionals are obliged to cooperate with the public prosecutor in investigating such cases.

The Commission de Surveillance du Secteur Financier (CSSF) is an independent government body under the jurisdiction of the Ministry of Finance that serves as the prudential oversight authority for banks, credit institutions, the securities market, some pension funds, and other financial sector entities covered by the country's anti-money laundering and terrorist financing laws. The Luxembourg Central Bank oversees the payment and securities settlement system, and the Commissariat aux Assurances (CAA), also under the Ministry of Finance, is the regulatory authority for the insurance sector. The identities of the beneficial owners of accounts are available to all entities involved in oversight functions, including registered independent auditors, in-house bank auditors, and the CSSF.

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

No distinctions are made in Luxembourg's laws and regulations between onshore and offshore activities. Foreign institutions seeking establishment in Luxembourg must demonstrate prior establishment in a foreign country and meet stringent minimum capital requirements. Companies must maintain a registered office in Luxembourg, and background checks are performed on all applicants. A ministerial decree published in July 2004 modified the Luxembourg Stock Exchange's internal regulations to make it easier to list offshore funds, provided the fund complies with CSSF requirements as detailed in Circular 04/151. Also, a government registry publicly lists company directors. Although nominee (anonymous) directors are not permitted, bearer shares are permitted. Officials contend that bearer shares do not present a problem for money laundering because of know-your-customer laws, requiring banks to know the identity of the beneficial owner. Banks must undergo annual audits under the supervision of the CSSF (CSSF reg. No. 27). Independent auditors have established a peer review procedure in compliance with an EU recommendation on quality control for external audit work to assure the adherence to international standards on auditing.

Established within Luxembourg's Ministry of Justice, the Cellule de Renseignement Financier (FIU-LUX) consists of two full and one part-time officials and serves as Luxembourg's FIU, receiving and analyzing STRs and seizing and freezing assets when necessary. As part of modifications made in 2004 to Luxembourg's money laundering law, the FIU's official status as a division within the Ministry of Justice Public Prosecutor's Office was formalized. As a result, FIU officials spend a fair proportion of their time on nonfinancial crime cases. Some members of the financial community continue to call for the creation of an administrative FIU body separate from the Office of the Public Prosecutor. The FIU is responsible for providing members of the financial community with access to updated information on money laundering and terrorist financing practices. It also works closely with various regulatory bodies such as the CSSF and the CAA. The FIU and CSSF work together in investigations involving significant money laundering cases. The FIU does not have direct access to the records or databases of other government entities, but the response to its requests have proven to be efficient.

In order to obtain a conviction for money laundering, prosecutors must now prove criminal intent rather than negligence. Negligence, however, is still scrutinized by the appropriate sector oversight authority, with sanctions for noncompliance varying from 1,250 to 1,250,000 euros.

In 2005, covered institutions filed a total of 831 STRs, compared to a total of 943 in 2004. This figure represents a slight decrease in comparison to the past two years (832 STRs were filed in 2003, 631 in 2002, and 431 in 2001). The rate of STR filings began to decrease as legislation was being introduced in 2004 to add professional obligations covered by the anti-money laundering and terrorist financing law. The majority of STRs still originate from banks. Of 388 confirmed cases of suspicious activity in 2005, including those received by international rogatory commission, 55 specifically related to money laundering, 30 to organized crime, 11 to drug-related money laundering, 5 to corruption, and 9 to other offenses. Among the 2,471 individuals involved in STRs in 2004, 383 were residents in Luxembourg, 350 in France, 333 in Belgium, 250 in Germany, 221 in Italy, 111 in the United Kingdom, 132 in Russia, and 71 in the United States. Statistics for 2006 are not available.

There has only been one money laundering case prosecuted in Luxembourg. The case is still pending. There is one additional money laundering case scheduled for trial in 2007.

Luxembourg law only allows for criminal forfeitures and public takings. Drug-related proceeds are pooled in a special fund to invest in anti-drug abuse programs. Funds found to be the result of money laundering can be confiscated even if they are not the proceeds of a crime. The GOL can, on a case-

by-case basis, freeze and seize assets, including assets belonging to legitimate businesses used for money laundering. The government has adequate police powers and resources to trace, seize, and freeze assets without undue delay. 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. On October 17, 2006, the United States and Luxembourg announced a sharing agreement in which they would divide equally €11,366,265.44 (approximately $ 14,548,820) of seized assets of two convicted American narcotics traffickers which had been domiciled in Luxembourg bank accounts. Reportedly, there is a consistently high level of cooperation between Luxembourg and other foreign countries' law enforcement authorities on money laundering investigations.

Luxembourg authorities have been actively involved in bilateral and international fora and training in order to become more effective at fighting the financing of terrorism. In July 2003, Luxembourg's parliament passed a multifaceted counterterrorism financing law known as Projet de Loi 4954, designed to strengthen Luxembourg's ability to fight terrorism and terrorist financing. The law defines terrorist acts, terrorist organizations, and terrorism financing in the Luxembourg Criminal Code. In addition, the specific crimes, as defined, will carry penalties of 15 years to life. The law also extends the definition of money laundering to incorporate new terrorism-related crimes and provides an exception to notification requirements in selected wiretapping cases. The November 2004 amendments bring Luxembourg into compliance with the FATF's Special Recommendation IV by extending the reporting obligations of the financial sector to terrorist financing, independently from any context of money laundering. Covered institutions now are required to report any transaction believed to be related to terrorist financing, regardless of the source of the funds.

The Ministry of Justice studies and reports on potential abuses of charitable and nonprofit entities to protect their integrity. 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 authorities have not found evidence of the widespread use in Luxembourg of alternative remittance systems such as hawala, black market exchanges, or trade-based money laundering. Officials comment that existing AML rules would apply to such systems, and no separate legislative initiatives are being formally considered to address them.

In an effort to identify and freeze the assets of suspected terrorists, 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 E.O. 13224. 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 some time now; however, the legislation remains in the early drafting process. Luxembourg's authorities can and do take action against groups targeted through the EU designation process and the UN.

Under the 2004 amendments to Luxembourg's AML law, bilateral freeze requests are limited to a new maximum of three months; designations under the EU, UN, or international investigation processes continue to be subject to freezes for an indefinite time period. Upon request from the United States, Luxembourg froze the bank accounts of individuals suspected of involvement in terrorism. Luxembourg has also independently frozen several accounts, resulting in court challenges by the account holders. Since 2001, over $200 million in suspect accounts have been frozen by Luxembourg authorities pending further investigations (most of the assets were subsequently released).

Luxembourg cooperates with and provides assistance to foreign governments in their efforts to trace, freeze, seize and forfeit assets. Dialogue and other bilateral proceedings between Luxembourg and the

United States have been extensive. Luxembourg held the EU Presidency from January through June 2005. As part of its presidency agenda, Luxembourg placed a priority on making progress on the additional legal instruments the United States had signed with the European Union covering extradition and mutual legal assistance. The extradition agreement will modernize existing bilateral extradition treaties with each of the EU member states. The mutual legal assistance agreement contains cutting-edge provisions for future legal cooperation, including the ability to informally identify the existence of bank accounts in terrorism-related cases. To implement the EU-wide agreements, supplemental treaties between the U.S. and each EU member states are required. On February 1, 2005, bilateral instruments were signed to implement the U.S.-EU extradition and mutual legal assistance agreements between Luxembourg and the United States. Luxembourg was instrumental in using its EU presidency to push this process closer to completion with four additional EU members as well.

In its 2005 EU Presidency capacity, Luxembourg also oversaw new milestones in the recently-established U.S.-EU dialogue on terrorist finance issues. Prosecutors and investigators from the United States and the EU's Eurojust met for the first time in March 2005 at The Hague to discuss a suspect terrorist group that operated in a number of countries. The Luxembourg EU Presidency hosted a two-day workshop in April 2005 for U.S. and EU member state terrorist finance prosecutors, investigators, and designators (who met for the first time at this event). The dialogue continued throughout 2005 to expand U.S.-Luxembourg and U.S.-EU cooperation between experts dedicated to countering terrorist financing. This forum was determined to be quite useful, and was continued by the Finnish EU Presidency as the second workshop was held 27-28 September 2006.

As of September 2005, over $22 million in illegal drug proceeds was frozen in Luxembourg at the request of U.S. authorities. Luxembourg worked with the United States Department of Justice throughout the year on several outstanding drug-related money laundering and asset forfeiture cases. On September 7, 2005, Luxembourg repatriated to the United States nearly $1 million, based on a U.S. legal assistance request, to victims of a fraud involving a former Vice President of Riggs Bank in Washington, D.C.

Luxembourg 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. The directive was published in the EU's Official Journal on November 25, 2005. EU member states must transpose this legislation into national law within the next two years.

Luxembourg is a party to the 1988 UN Drug Convention and but has not yet ratified the UN Convention against Transnational Organized Crime. In November 2003, Luxembourg ratified the UN International Convention for the Suppression of the Financing of Terrorism.

Luxembourg is a member of the European Union and the FATF. The Luxembourg FIU is a member of the Egmont Group and has negotiated memoranda of understanding with several countries, including Belgium, Finland, France, Korea, Monaco, and Russia. Luxembourg and the United States have had a mutual legal assistance treaty (MLAT) since February 2001. Luxembourg's Agency for the Transfer of Financial Technology (ATTF) has consistently provided training and acted as a consultant in money laundering matters to government and banking officials in countries whose regimes are in the development stage. Since 2001, ATTF has provided assistance to government and banking officials from Bosnia-Herzegovina, Bulgaria, Croatia, Cape Verde, China, the Czech Republic, Egypt, Macedonia, Romania, Russia, Ukraine, Cyprus, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia and Slovenia, El Salvador, Kazakhstan, Laos, Moldova, Mongolia, Serbia and Montenegro,

Tunisia, Turkey, Uzbekistan, and Vietnam. Georgia was added to this list in 2006 and the hope is to add Azerbaijan in 2007.

According to the December 2004 International Monetary Fund (IMF) report Luxembourg: Report on the Observance of Standards and Codes—FATF Recommendations for Anti-Money Laundering and Combating the Financing of Terrorism, Luxembourg has "a solid criminal legal framework and supervisory system" to counter money laundering and terrorist financing and is "broadly compliant with almost all of the Financial Action Task Force (FATF) Recommendations." The report also notes that Luxembourg's high level of cross-border business, obligatory banking secrecy, private banking, and "certain investment vehicles" create a challenging environment for countering money laundering and terrorist financing

The Government of Luxembourg has enacted laws and adopted practices that help to prevent the abuse of its bank secrecy laws, and it has enacted a comprehensive legal and supervisory anti-money laundering regime. However, further action should be taken to address the lack of a distinct legal framework for the financial intelligence unit. The financial intelligence unit staff should have its other judicial responsibilities curtailed and be freed to focus solely on financial crimes. Regarding regulations, Luxembourg should continue to strengthen enforcement to prevent abuse of its financial sector. Specifically, Luxembourg should pass legislation creating the authority for it to independently designate those who finance terrorism. Luxembourg should also enact legislation to address the continued use of bearer shares. Per FATF Special Recommendation Nine, Luxembourg should initiate and enforce cross-border currency reporting requirements and the data should be shared with the financial intelligence unit. Luxembourg's anti-money laundering regime may be relying too heavily on the filing of suspicious transaction reports to generate investigations. Although Luxembourg has steadily enacted anti-money laundering and terrorist finance laws, policies, and procedures, the lack of prosecutions and convictions is telling, particularly for a country that boasts such a large financial sector.

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 except defense and foreign affairs. Macau's free port, lack of foreign exchange controls, and significant gambling industry create an environment that can be exploited for money laundering purposes. In addition, 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 has a small economy heavily dependent on gaming, but is emerging as a financial center. Its offshore financial sector is not fully developed.

Main money laundering methods in the financial system are wire transfers; currency exchange/cash conversion; the use of casinos to remit or launder money; and the use of nominees, trusts, family members, or third parties to transfer cash. 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, calls for the establishment of a financial intelligence unit (FIU), and includes provisions on due diligence. The 2006 anti-money laundering law broadened the definition of money laundering to include all serious predicate crimes. 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, the penalties would increase by one-half. The new law also allows for fines to be added to the time served and eliminated a provision reducing time served for good behavior.

The 2006 law also extended 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 to send suspicious transaction reports (STRs) to the relevant authorities and cooperate in any follow-up investigations. This law also requires casinos to submit STRs.

On March 30, 2006, the MSAR also passed new counterterrorism legislation aimed at strengthening measures to combat the financing of terrorism (CFT). The law generally complies with UNSCR 1373, 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 stiffer penalties. However, the draft legislation does not mention how to freeze without delay terrorist assets, nor does it discuss international cooperation on terrorism 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.

While Macau's new AML and CTF laws should create a more robust legal framework to combat money laundering, Macau will also need to enforce these laws. In an August 2002 "Assessment of the Regulation and Supervision of the Financial Sector of Macao", the IMF concluded that Macau was "materially noncompliant" with the Basel Committee's anti-money laundering principles, and recommended a number of improvements. On September 15, 2005, the U.S. Department of Treasury designated Macau-based Banco Delta Asia as a primary money laundering concern under the USA PATRIOT Act. According to the U.S. Treasury Department, Banco Delta Asia provided financial services for more than 20 years to North Korea and facilitated many of that regime's criminal activities, including circulating counterfeit U.S. currency. Macau's Monetary Authority has taken control of Banco Delta Asia and is cooperating with the U.S. Treasury Department in an ongoing investigation of the bank.

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. One of its key functions is to receive all suspicious transaction reports (STRs) in Macau and to undertake subsequent investigations. 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.

Macau is in the process of establishing a Financial Intelligence Unit (FIU). A Macau Monetary Authority official has been designated to head the FIU. As of October 2006, 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 is working on creating an operations manual, and is working with the Macau Police on dissemination of suspicious transaction reports (STRs) and with the Public Prosecutors Office on prosecution of cases. The FIU is currently working out of temporary office space but plans to move into permanent office space in January 2007 when it will begin accepting STRs.

The gaming sector and related tourism are critical parts of Macau's economy. Taxes from gaming comprised 73 percent of government revenue in the first eight months of 2006. Gaming revenue increased 12.6 percent during the first eight months of 2006, compared with a year earlier. The MSAR ended a long-standing gaming monopoly early in 2002 when it awarded concessions to two additional operators, the U.S.-based Venetian and Wynn Corporations. . Macau now effectively has six separate casino licenses, three concession holders Sociedade de Jogos de Macau (SJM), Galaxy and Wynn and three subconcession holders Las Vegas Sands, MGM and PBL/Melco. Las Vegas Sands opened its first casino, the Sands, on May 18, 2004. In addition, MGM began constructing a casino in conjunction with Pansy Ho, the daughter of local businessperson Stanley Ho, the largest casino operator in Macau, whose company, Sociedade de Jogos de Macau (SJM), previously held a monopoly on casino operations. Wynn opened its casino in September 2006 and MGM and the Venetian are scheduled to open casinos in 2007. A consortium between Australia's PBL and Macau's Melco, led by Stanley Ho's son Lawrence Ho, as yet operates no casinos, but runs several slot machine rooms in Macau.

Under the old monopoly framework, organized crime groups were, and continue to be, 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 were shielded from 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. Unlike SJM and new entrant Galaxy, the Sands does not cede control of its VIP gaming facilities to outside organizations. This approach impedes organized crime's ability to penetrate the Sands operation.

The MSAR's money laundering legislation includes provisions designed to prevent money laundering in the gambling industry. The legislation aims to make money laundering by casinos more difficult, improve oversight, and tighten 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 by outsiders. The law requires both casinos and junket operators to register with the government.

Terrorist financing is criminalized under the Macau criminal code (Decree Law 58/95/M of November 14, 1995, Articles 22, 26, 27, and 286). The MSAR has the authority to freeze terrorist assets, although a judicial order is required. Macau financial authorities directed 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 assets were identified in 2005.

The Macau legislature passed a counterterrorism law in April 2002 that is intended to assist with Macau's compliance with UNSCR 1373. The legislation criminalizes violations of UN Security Council resolutions, including counterterrorism resolutions, and strengthens counterterrorist financing provisions. China signed the UN International Convention for the Suppression of the Financing of Terrorism on November 13, 2001, and the Standing Committee of the 10th National People's Congress ratified it in February 2006. The Instrument of Ratification was delivered to the UN on April

21, 2006, and stipulated that in accordance with Article 138 of the Basic Law of the Macao Special Administrative Region of the People's Republic of China, the Government of the People's Republic of China had decided that the Convention shall apply to the MSAR.

The increased attention paid 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 low. Macau's Judiciary Police received 107 STRs in 2003, 109 in 2004, 194 in 2005, and 396 STRs from January to September of 2006, from individuals, banks, companies, and government agencies. In 2003 Macau opened two money laundering cases and prosecuted one. In 2004 Macau opened ten money laundering cases and prosecuted zero. In 2005 Macau opened nine money laundering cases and prosecuted two. In the first half of 2006 Macau opened twelve money laundering cases and prosecuted one. 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, money changers, and remittance agents, addressing record keeping and suspicious transaction reporting for cash transactions over $2,500. For such transactions, banks, insurance companies, and moneychangers must perform customer due diligence. In 2003, the Macau Monetary Authority examined all money changers 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.

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.

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's Monetary Authorities are cooperating with the U.S. Treasury Department investigation of Banco Delta Asia. The Monetary Authorities have taken control of Banco Delta Asia and have frozen accounts linked to North Korea worth approximately US$ 24 million. The Government of Macau announced in September 2006 that it would continue to maintain control over Banco Delta Asia for at least six more months as the Banco Delta Asia investigation continues.

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 September 2003, Macau became a party to the UN Convention against Transnational

Organized Crime as a result of China's ratification. Macau also became a party to the 1988 UN Drug Convention through China's ratification. Macau has taken a number of steps in the past three years to raise industry awareness of money laundering. During a March 2004 IMF technical assistance mission, the IMF and Monetary Authority of Macau organized a seminar for financial sector representatives on the FATF Revised Forty Recommendations. The Macau Monetary Authority trains banks on anti-money laundering measures on a regular basis.

Macau should implement and enforce existing laws and regulations, and ensure effective implementation of its new legislation. Macau should ensure that regulations, structures, and training are put in place to prevent money laundering in the gaming industry, including implementing as quickly as possible regulations to prevent money laundering in casinos, including the VIP rooms. The MSAR should take steps to implement the new FATF Special Recommendation Nine, 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 increase public awareness of the money laundering problem, improve interagency coordination, and boost cooperation between the MSAR and the private sector in combating money laundering. The Government of Macau should ensure that its financial intelligence unit meets Egmont Group standards for information sharing. It should expedite the drafting and issuance of implementing regulations to its new AML and CTF laws. The Government of Macau also should be more proactive in identifying and freezing accounts related to money laundering by weapons proliferators and counterfeiters.

Malaysia

Malaysia is not a regional center for money laundering. However, its financial sectors are vulnerable to abuse by narcotics traffickers, financiers of terrorism, and criminal elements. Malaysia's relatively lax customs inspection at ports of entry and free trade zones, and its offshore financial services center serve to increase its vulnerability. Though the Government of Malaysia (GOM) has established a "drug-free by 2015" policy and cooperation with the U.S. on combating drug trafficking is excellent, Malaysia's proximity to the heroin production areas and methamphetamine labs of the Golden Triangle leads to smuggling across Malaysian borders, destined for Australia and other markets. Ecstasy from Amsterdam is flown into Kuala Lumpur International Airport for domestic use and distribution to Thailand, Singapore, and Australia.

Malaysia, having enacted laws to combat money laundering, has a developed anti-money laundering system. Malaysia has endorsed the Basel Committee's Core Principles for Effective Banking Supervision, and generally follows international standards related to money laundering, including the Financial Action Task Force (FATF) Forty Recommendations on Money Laundering and the Nine Special Recommendations on Terrorist Financing. 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 2001 (AMLA). The NCC also coordinates government-wide anti-money laundering and counterterrorist finance efforts.

Malaysia is a member of the Asia/Pacific Group on Money Laundering (APG),. In 2001, the APG conducted a Mutual Evaluation of Malaysia and its offshore financial center, Labuan. The second round of evaluations is scheduled in February 2007. In preparation for the APG's second round, the NCC has established various working groups to review Malaysia's current anti-money laundering and counter terrorist finance (AML/CTF) measures, laws, regulations, guidelines and framework in an effort to identify possible gaps and to formulate corrective measures.

Subsequent to its 2001 mutual evaluation, Malaysia enacted the AMLA in January 2002, criminalizing money laundering and lifting bank secrecy provisions for criminal investigations involving more than 122 predicate offenses. In 2005, the number of money laundering predicate offences in the Second Schedule to the AMLA was increased from 168 to 185 serious offences from 27 pieces of legislation.

The new predicate offenses were from the Customs Act, Islamic Banking Act, Payment Systems Act, Takaful Act, Futures Industry Act, Securities Commission Act and the Securities Industry Act.

The AMLA also created a financial intelligence unit (FIU), the Unit Perisikan Kewangan, located in the Central Bank, Bank Negara Malaysia (BNM). The FIU is tasked with receiving and analyzing information, and sharing financial intelligence with the appropriate enforcement agencies for further investigations. The Malaysian FIU 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. Currently, BNM maintains 300 examiners who are responsible for money laundering inspections for both onshore and offshore financial institutions. Malaysia's FIU has been a member of the Egmont Group since July 2003. This year Malaysia was elected to be the Asia Chair for the Egmont Committee.

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 Malaysia's FIU. If the reporting institution deems a transaction suspicious it must report that transaction to the FIU regardless of the transaction size. In addition, cash threshold reporting (CTR) requirements above approximately $13,600 were invoked on banking institutions. FIU 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 waived in the case of money laundering investigations.

Malaysia has adopted banker negligence (due diligence) laws that make individual bankers responsible if their institutions launder money. 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, is subject to criminal sanction. All reporting institutions are subject to review by the FIU. 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, accountants, company secretaries, and Malaysia's one licensed casino. In 2005, reporting obligations were invoked on 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.

According to a Ministry of Finance report released in September 2006, Islamic banking assets accounted for 11.8 percent of the total assets in the banking sector at the end of June 2006, up from 11.6 percent in June 2005. Malaysia's Islamic finance sector is subject to the same strict supervision to combat financial crime as the commercial banks. A combination of legacy exchange controls imposed after the 1997-98 Asian financial crisis in addition to robust regulation and supervision by BNM makes the Islamic financial sector as unattractive to financial criminals as is the conventional financial sector.

In 1998 Malaysia imposed foreign exchange controls that restrict the flow of the local currency from Malaysia. Onshore banks must record cross-border transfers over approximately $1,360. Since April 2003, an individual form is completed for each transfer above approximately $13,600. Recording is done in a bulk register for transactions between approximately $1,411 and $14,110. 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 5,408 registered offshore companies as of June 30, 2006, of which 256 had registered since January this year. 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." Eleven days later, 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. Legal treatment for such zones is also different. The time needed to obtain such licenses from the administrative authority for the given free trade zone depends on the type of approval. Clearance time ranges from two to eight weeks. There is no information available suggesting that Malaysia's free industrial and free commercial zones are being used for trade-based money laundering schemes or by the financiers of terrorism. However, the Government of Malaysia (GOM) considers these zones as areas outside the country and they receive lenient tax and customs treatment relative to the rest of the country.

In April 2002, the GOM passed the Mutual Assistance in Criminal Matters Bill, 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.

In 2004, Malaysia made its first money laundering arrest. As of December 31, 2005, six individuals were being prosecuted for money laundering offences involving a total of 196 charges with fines amounting to approximately $19.5 million. In December 2005, one person was convicted of a money laundering offence amounting to approximately $23,423. From January through November 2006, 14 additional individuals had been charged, bringing the total number of people being prosecuted for money laundering to 20 with fines amounting to approximately $71.97 million.

Malaysia cooperates with regional, multilateral, and international partners to combat financial crimes and permits foreign countries to check the operations of their bank branches.

The FIU has signed memoranda of understanding (MOUs) on the sharing of financial intelligence with the FIUs of Australia, Indonesia, Thailand, the Philippines and China. MOUs with the United Kingdom, United States, Japan, South Korea, Netherlands Antilles, Finland, Albania, Argentina, Cook Islands, Mexico, Sri Lanka, Ukraine, Peru and India are at various stages of negotiation.

Malaysia is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. The GOM has agreed in principle to accede to the UN Convention for the Suppression of the Financing of Terrorism, and is expected to bring into force amendments to five different pieces of legislation. Parliament passed amendments to the Anti-Money Laundering Act, the Penal Code, the Subordinate Courts Act, the Courts of Judicature Act, and the Criminal Procedure Code. All five amendments have been accorded Royal Assent and are awaiting Ministerial instructions to bring these amendments into force. These amendments will increase 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.

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 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 has issued orders to all licensed financial institutions, both onshore and offshore, to do so. The Ministry of Foreign Affairs opened the Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT) in August 2003. The SEARCCT has hosted a series of counterterrorism courses and seminars, including training on counter terrorist finance.

BNM and SEARCCT jointly organized a series of workshops and dialogues for reporting institutions with the participation of regulatory and law enforcement agencies. Malaysia offers interactive computer-based training in anti-money laundering developed by the UN Office on Drugs and Crime and the World Bank. In addition, BNM together with members of the NCC has developed an eight-module Accreditation of Financial Investigators Program for AMLA investigators. Ongoing training enhances the capabilities of graduates of the computer-based programs, including the legal aspects of anti-money laundering, investigative procedures, analysis of net worth, forensic accounting, and computer forensics.

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 submits its annual returns, including its financial statements. Should activities deemed suspicious be found, the Registrar may revoke the nonprofit organization's (NPO) registration or file a suspicious transaction report. Registering 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 54 cents and annual financial statements. In

March 2006, the FIU completed a review of the nonprofit sector with the Registrar, the IRB, and CCM in an effort to ensure that the laws and regulations were adequate to mitigate the risks of nonprofit organizations as conduits for terrorism 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 for contributions to mosques or Islamic charitable organizations (zakat, as required by Islam) encouraging the reporting of such contributions. There is no similar tax credit for non-Muslims. Islamic zakat contributions can be taken as payroll deductions, adding another tool to help prevent the abuse of charitable giving.

The FIU has provided capacity building and training in anti-money laundering efforts to some of its ASEAN partners, including Cambodia, Laos, and Vietnam. In February 2006, the Asian Development Bank (ADB) funded a team from Malaysia's FIU to run a workshop in Laos for two state-owned banks and to provide technical assistance in the drafting of Laos's anti-money laundering compliance procedures. This was completed in October 2006.

The Malaysian government continues to receive training towards the more effective use of existing "Aiding and Abetting" laws to prosecute drug kingpins and their organizations.

The Government of Malaysia (GOM) should enact an imminent effective date for the five recent amendments criminalizing the financing of terrorism. This also will allow Malaysia to accede to the UN International Convention for the Suppression of the Financing of Terrorism. Malaysia also should continue to enhance its cooperation with 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. Perhaps most importantly, the GOM should implement stricter border control measures.

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 believed to be the principal source of funds laundered through the Mexican financial system. Corruption, kidnapping, trafficking in firearms and immigrants, and other crimes are other major sources of illegal proceeds being laundered. 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. Mexico's financial institutions are vulnerable to currency transactions involving international narcotics trafficking proceeds that include significant amounts of U.S. currency derived from illegal drug sales in the United States.

Currently, there are 29 commercial banks and 71 foreign financial representative offices operating in Mexico, as well as 86 insurance companies, 166 credit unions and 25 money exchange houses. 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 narcotics-driven segments of the economy.

Beginning in 2005, permits were issued for casinos to operate in Mexico. Gambling is also legally allowed through national lotteries, horse races and sport pools. Casinos, offshore banks, lawyers, accountants, couriers and brokers are currently not subject to anti-money laundering (AML) reporting requirements.

In 2005, Mexico established three strategic financial zones: two in San Luis Potosi and one in Chiapas. These zones, similar to free trade zones, allow tax exemptions for inputs to exports that are imported

or produced locally. Additional strategic financial zones are planned to be established in the states of Queretaro, Quintana Roo and Lazaro Cardenas. The Mexican Customs agency certifies companies operating in these zones under the authority provided by Article 135 of the Customs Law. There is no indication that these zones are being used in trade-based money laundering or terrorist financing.

Since 2000, Mexicans have received more than $100 billion in remittances. Approximately $23.1 billion in remittances were received in 2006 alone. 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." The matricula consular is 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 and pay a flat fee to receive a remittance; neither is required to open a bank account in the United States or Mexico. Although these systems have been designed to make the transfer of money faster and less expensive for the customers, the rapid movement of such vast sums of money by persons of questionable identity leaves the systems open to potential money laundering and exploitation by organized crime groups. As a result of the increased availability of these electronic transfers, the U.S. embassy estimates that electronic transfers accounted for 90 percent of remittances to Mexico in 2006.

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. Sophisticated and well-organized drug trafficking organizations based in Mexico are able to take full advantage of the extensive United States-Mexico border and the large flow of licit remittances. In addition, the combination of a sophisticated financial sector and weak regulatory controls facilitates the concealment and movement of drug proceeds. U.S. officials estimate that since 2003, as much as $22 billion may have been repatriated to Mexico from the U.S. by drug trafficking organizations. In April 2006, the U.S. Department of Treasury issued a warning to the U.S. financial sector on the potential use of certain Mexican financial institutions, including Mexican casas de cambio, 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.

In 2006, U.S. authorities observed a significant increase in the number of complex money laundering investigations by the Financial Crimes Unit of the Office of the Deputy Attorney General Against Organized Crimes (SIEDO), including cases coordinated with U.S. officials. As a result of the cooperation of Mexican Customs, SIEDO and various U.S. agencies, Mexico seized over $25 million in 2006. As of November, SIEDO had initiated 142 criminal investigations into money laundering cases in 2006, 77 of which were brought to trial. The U.S. Treasury Department's Office of Foreign Asset Control (OFAC) announced in June 2006 the designation of the Amezcua Contreras Organization as a Tier I target involved in significant narcotics trafficking under the Foreign Narcotics Kingpin Designation Act. In July and September 2006, OFAC also announced designations of 45 Tier II targets associated with the previously-designated Arrellano Felix and Arriola Marquez drug trafficking organizations. The designations are a result of cooperation among OFAC, other U.S. government entities and SIEDO. They allow U.S. and Mexican authorities to seek the freezing of assets of Mexican drug cartels, hindering their ability to take advantage of the U.S. and Mexican financial systems.

The Government of Mexico (GOM) continues its efforts to create and implement an anti-money laundering program that meet such international standards as those of the Financial Action Task Force (FATF), which Mexico joined in June 2000. Money laundering related to all serious crimes was criminalized in 1996 under Article 400 bis of the Federal Penal Code and is punishable by imprisonment of from 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.

In 1997, the GOM established a financial intelligence unit under the Ministry of the Treasury, which became known as the Unidad de Inteligencia Financiera (UIF) in 2004 with the consolidation of all the Treasury offices responsible for investigating financial crimes into the UIF. The UIF is responsible for receiving, analyzing and disseminating financial reports from a wide range of obligated entities. The UIF also reviews all crimes linked to Mexico's financial system and examines the financial activities of public officials. The UIF's personnel number approximately 70 and are comprised mostly of forensic accountants, lawyers and analysts. Its director reports to the Minister of Finance.

Regulations have been implemented for banks and other financial institutions (mutual savings companies, insurance companies, financial advisers, stock markets, credit institutions, exchange houses and money remittance businesses) to know and identify customers and maintain records of transactions. These entities must report to the UIF any suspicious transactions, transactions over $10,000, and transactions involving employees of financial institutions who engage in unusual activity. Financial institutions with a reporting obligation also require occasional customers performing transactions equivalent to or exceeding $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). Financial institutions also have implemented programs for screening new employees and verifying the character and qualifications of their board members and high-ranking officers. Real estate brokerages, attorney, notaries, accountants and dealers in precious metals and stones are required under a November 2005 provision of the tax law to report all transactions exceeding $10,000 to the UIF, via the Tax Administration Service (SAT). As of 2006, nonprofit organizations are also subject to reporting requirements on donations greater than $10,000. In 2005, the UIF received over 4 million CTRs and approximately 57,700 STRs from obligated entities; corresponding data for 2006 is not available.

In December 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 $10,000 or more. These reports are also received by the UIF and cover a wider range of monetary instruments (e.g. bank drafts) than those required by the United States.

Following the analysis of CTRs, STRs and reports on the cross-border movements of currency, the UIF sends reports that are deemed to require further investigation, and have been approved by Treasury's legal counsel, to the Office of the Attorney General (PGR). As of October, the UIF had sent 45 cases to the PGR in 2006. The PGR's special financial crimes unit is part of SIEDO, which works closely with the UIF in carrying out money laundering investigations. In addition to working with SIEDO, UIF personnel have initiated working-level relationships with other federal law enforcement entities, including the Federal Investigative Agency (AFI) and the Federal Preventive Police (PFP), in order to support the investigations of criminal activities with ties to money laundering. In 2006, the UIF signed memoranda of understanding (MOUs) with the Economy Secretariat and the immigration authorities that allows the UIF access to their databases. The UIF has also signed agreements with the National Banking Commission (CNBV) and the National Commission of Insurance and Finance (CNSF) to coordinate methods to prevent money laundering and terrorist financing, and is currently finalizing similar negotiations with the Treasury and the National Savings Commission (CNSAR).

Since undergoing its second mutual evaluation by the FATF in 2003, the GOM has been subject to monitoring by FATF and has submitted several reports on the progress made since its evaluation. The evaluation team found in 2003 that the GOM had made progress since the first mutual evaluation by removing specific exemptions to customer identification obligations, implementing on-line reporting

forms and a new automated transmission process for reporting transactions to the UIF, reducing the delay in reporting transactions overall, and developing an overall anti-money laundering strategy. However, the FATF evaluation team also identified a number of deficiencies in the system. These deficiencies include the lack of a separate criminal offense of terrorist financing, and strict bank and trust secrecy, which are considered impediments to investigations and prosecutions. As a result of these deficiencies, the GOM must update the FATF on its progress, which it did at the June and October 2005 and February 2006 plenary meetings of the FATF.

While Mexico has not yet criminalized terrorist financing, it has made improvements to its bank secrecy laws. Amendments to the Banking Law approved in April and December 2005 now allow specific government entities, such as the PGR and the state attorneys general, to receive records directly from banks and credit institutions without prior approval from the CNBV. Financial institutions must respond to these requests within three days.

In November 2003, the Senate passed a bill amending the Federal Penal Code that would link terrorist financing to money laundering. However, the lower house failed to act on this bill. In 2005, the draft legislation was re-submitted as two separate draft laws: one to criminalize the financing of terrorism and one to address outstanding international cooperation issues. If passed, this legislation would bring Mexico into compliance with international standards. The proposed amendments would also create two new crimes: conspiracy to launder assets and international terrorism (when committed in Mexico to inflict damage on a foreign state). The draft legislation is still under consideration in the Senate.

While Mexico does not have a specific offense criminalizing the financing of terrorism, money laundering associated with terrorism is punishable under the existing Penal Code. The GOM has responded positively to U.S. Government efforts to identify and block terrorist-related funds. It continues to monitor suspicious financial transactions, although no assets related to terrorism have been frozen to date.

Although the United States and Mexico both have 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 not often met with success. Mexican authorities have difficulties forfeiting assets seized in Mexico if these assets are not clearly linked to narcotics. Although Mexican officials have made significant progress in modernizing their approach to asset seizure, actual asset forfeiture remains a challenge.

Mexico has developed a broad network of bilateral agreements and regularly meets in bilateral law enforcement working groups with the United States. The U.S.-Mexico Mutual Legal Assistance Treaty 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. In addition to its membership in the FATF, Mexico participates in the Caribbean Financial Action Task Force as a cooperating and supporting nation. In 2006, Mexico also became a member of the South American Financial Action Task Force (GAFISUD), after previously participating in GAFISUD as an observer member. The UIF is a member of the Egmont Group, and Mexico participates in the 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 UIF has signed memoranda of understanding for the exchange of information with 22 other financial intelligence units, including the U.S. financial intelligence unit, FinCEN.

To create a more effective AML regime, Mexico should fully implement and improve its mechanisms for asset forfeiture and money laundering cooperation with the United States and increase efforts to

control the bulk smuggling of currency across its borders. The GOM should also closely monitor remittance systems for possible exploitation by criminal or terrorist groups. Mexico should enact its proposed legislation to criminalize the financing and support of terrorists and terrorist organizations. Despite a strengthened regulatory framework, improved cooperation among law enforcement authorities and a strong public campaign against corruption, Mexico continues to face challenges in prosecuting and convicting money launderers, and should continue to focus its efforts on improving its ability to combat money laundering, terrorist financing and other financial crimes.

Moldova

Moldova is not considered an important regional financial center. Moldova remains predominantly a cash-based society and people reportedly have little faith in banks. Criminal proceeds laundered in Moldova are derived from both domestic and foreign criminal activity. Organized crime syndicates are active in the country. Widespread corruption in both commerce and government exacerbates the situation. There is a large underground economy in Moldova. Smuggling of consumer goods, including counterfeit items, is common. Moldova is also recognized as a major source country for trafficking in persons. A rise in internet-related fraud schemes is evident. Moldova has approximately five casinos, but they are neither well regulated nor controlled.

Additional money laundering threats are found in the separatist region of Trans-Dniester—a narrow strip of land between the Dniester River and the Ukrainian border—which proclaimed independence from Moldova in 1990. Trans-Dniester contains most of Moldova's industrial infrastructure, but its economic potential is limited by its international isolation. The region is plagued by corruption, organized crime and smuggling. There are persistent reports of Trans-Dniester illegal arms sales, narcotics trafficking, and of being the base of operations for Russian and Ukrainian organized crime syndicates.

Money laundering became a criminal offense in Moldova November 2001, and the law was amended in June 2002. It remained unchanged when the new criminal code was adopted in June 2003. The legislation applies to proceeds of "all crimes," not just narcotics activity, with banks and nonbank financial institutions (NBFIs) required to report transactions over a certain amount to the Center for Combating Economic Crimes and Corruption (CCECC). On July 1, 2004, the Law on Money Laundering was amended to raise the reporting threshold from 100,000 lei to 300,000 lei (approximately $8,040 to $24,100) for individuals, and from 200,000 lei to 500,000 (approximately $16,100 to $40,200) for legal entities. However, the amendments still require reporting transactions under the threshold if, when combined with other transactions during a one-month period, they reach a total which crosses that threshold. This amendment may actually increase the amount of reporting required. Current anti-money laundering legislation also covers gold, gems, and precious metals.

Banks must maintain transfer records for a period of five years after an account opens or after any financial transaction takes place and seven years after foreign currency contract transactions, whichever is later. They have submitted suspicious transactions reports (STRs), as required, since the law was enacted. However, Moldovan legislation exempts foreign nationals from being subject to STR reporting. Both banks and NBFIs are protected from criminal, civil, and administrative liability asserted as a result of their compliance with the reporting requirements, and no secrecy laws exist that would prevent law enforcement or banking authorities from accessing financial records. A May 2003 amendment states that forwarding such information to law enforcement entities or the courts is not a breach of confidentiality, as long as it is done in accordance with the regulations. Current legislation contains provisions authorizing sanctions of commercial banks for negligence.

Government of Moldova (GOM) efforts against the international transportation of illegal-source currency and monetary instruments largely focus on cross-border currency reporting forms, completed at ports of entry by travelers entering Moldova. It is not clear if these efforts are successful.

The CCECC houses Moldova's Financial Intelligence Unit (FIU). In 2004, the CCECC established an FIU from within, by creating a money laundering section of ten investigators to pursue suspicious financial transactions. Under Moldovan criminal procedure, cases first undergo a preliminary investigation by operative investigators before being sent to criminal investigators and prosecutors who decide whether a full investigation will be launched. The FIU is not a member of the Egmont Group, although it has been a candidate for membership since 2004. Reportedly, the FIU has drafted a new anti-money laundering/counterterrorist financing (AML/CTF) law, which is to be submitted to Parliament in early 2007. The legislation was developed with technical assistance from the Council of Europe.

Moldova is not considered an offshore financial center, and only two foreign banks exist in Moldova: "Banca Comerciala Romana," a Romanian bank; and "Unibank," in which the Russian bank "Petrocomert" holds 100 percent of the shares. These banks are regulated in the same manner as Moldovan commercial banks. Offshore banks are permitted, so long as they are licensed and background checks are conducted on shareholders and bank officials. Nominee (anonymous) directors are not allowed, and banks do not permit bearer shares. The Ministry of Finance (MOF) currently licenses five casinos, although they are reportedly not well regulated or controlled.

Reportedly, the GOM is seriously considering a package of amendments to existing legislation that would allow Moldova to emerge as a significant offshore center in the region. The GOM has indicated publicly that the proposed changes are designed to attract substantial inflows of capital and provide a much-needed economic boost to one of the poorest countries in Europe. According to the current draft of the proposed amendments, the changes call for a sharp decrease in reporting requirements and an increase in financial secrecy, including the ability to establish "anonymous" stock companies. As drafted, neither banks nor law enforcement would be able to determine the beneficial owner of legal entities, and the law would provide what would effectively equate to a fee schedule for the "legalization" of money of dubious origin. If passed in their current form, the amended laws would violate FATF recommendations and call into question Moldova's compliance with and commitment to international AML/CFT standards.

Article 106 of the Moldovan criminal code, enacted June 12, 2003, relates specifically to asset seizure and confiscation. The article, titled "Special Seizures," describes a special seizure as the forced transfer of ownership of goods used during, or resulting from, a crime to the state. The article may be applied to goods belonging to persons who knowingly accept assets acquired illegally, even when prosecution is declined. However, it remains unclear whether asset forfeiture may be invoked against those unwittingly involved in or tied to an illegal activity. Money laundering crimes are the purview of the CCECC, while narcotics-related seizures are within the jurisdiction of the Ministry of Interior (MOI). The GOM currently lacks adequate resources, training, and experience to trace and seize assets effectively. There are no accurate statistics available on seizures or confiscation.

Moldova codified the criminalization of terrorist financing in the Law on Combating Terrorism, enacted November 12, 2001. Article 2 defines terrorist financing, and Article 8/1 authorizes suspension of terrorist and related financial operations. Current GOM capabilities to identify, freeze, and seize terrorist assets are rudimentary, with investigators lacking advanced training and resources. While the NBM receives and regularly distributes the UNSCR 1267 Sanctions Committee's consolidated list of suspected terrorists, no related assets have been identified, frozen, or seized in Moldova. Investigation into misuse of charitable or nonprofit entities is non-existent, as the GOM has neither the resources nor ability to perform these tasks. In December 2004, the Parliament amended the law on money laundering to include provisions on terrorist financing. Moldova has made no arrests for terrorist financing. Moldova is a party to the UN International Convention for the Suppression of the Financing of Terrorism.

No agreements, bilateral or otherwise, exist between the USG and the GOM regarding the exchange of records in connection with narcotics, terrorism, terrorist financing, or other serious criminal

investigation. Current legislation does not prohibit cooperation on a case-by-case basis. GOM authorities continue to solicit USG assistance on individual cases and cooperate with U.S. law enforcement personnel when presented with requests for information/assistance. There are no known cases of GOM refusal to cooperate with foreign governments or of sanctions or penalties being imposed upon the GOM for a failure to cooperate.

Moldova is a party to the 1988 UN Drug Convention and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime. 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 and as a candidate in the Egmont Group. Moldova is a member of the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL).

In December, 2006 Moldova signed a $24.7 million Threshold Country Program with the Millennium Challenge Account that focuses on anticorruption measures. The GOM requested funding to address areas of persistent corruption including in the judiciary, health care system, and tax, customs and police agencies. Moldova is listed as 79 out of 163 countries in Transparency International's 2006 Corruption Perception Index.

The Government of Moldova should enhance its existing anti-money laundering/counterterrorist financing regime. The regime should adhere to internationally accepted standards. Moldova should improve the mechanisms for sharing information and forfeiting assets. Additionally, Moldova should provide appropriate training for its law enforcement personnel involved in the asset forfeiture program. Border enforcement and antismuggling enforcement should be priorities. Moldova should take specific steps to counter corruption and should become a party to the UN Convention on Transnational Organized Crime and the UN Convention against Corruption. Moldova should not pursue proposed legislative changes on offshores that would make Moldova's financial sector less transparent and more vulnerable to money laundering, terrorist financing, and other forms of illicit finance. As a member of MONEYVAL, the Government of Moldova has committed to adhering to the international standards set by the Financial Action Task Force to combat money laundering and terrorist financing. Establishing an offshore shore financial sector would belie that commitment.

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 reportedly does not face the ordinary forms of organized crime, and the crime that does exist does not seem to generate significant illegal proceeds, with the exception of fraud and offenses under the "Law on Checks." Monaco remains on an 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 $91 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 four 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 concentrates on portfolio management and private banking. Subsidiaries of foreign banks operating in Monaco may withhold customer information from the parent bank.

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

Money laundering in Monaco has been criminalized by 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.

The original AML legislation requires banks, insurance companies, and stockbrokers to report suspicious transactions 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.

The 2002 amendments to Act 1.162 expanded the scope of AML reporting requirements to include corporate service providers, portfolio managers, some trustees, and institutions within the offshore sector. The Act instituted new procedural requirements regarding internal compliance, client identification, and records retention and maintenance. Sovereign Order 16.615 of January 11, 2005, and Sovereign Order 631 of August 10, 2006, mandate additional customer identification measures.

Offshore companies are subject to the same due diligence and suspicious reporting obligations as banking institutions, and Monegasque authorities conduct on-site audits. The 2002 legislation strengthened 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 financial intelligence unit (FIU), but also to implement internal AML and counterterrorist financing (CTF) procedures. The FIU monitors these activities.

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.

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

Monaco's FIU, known in French as 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 Law 1.162, Article 4, 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 2005. In 2005, SICCFIN received 375 STRs, about 60 percent of which were submitted by banks and other financial institutions. SICCFIN received 63 requests for financial information from other FIUs in 2005.

Investigation and prosecution 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 in 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 $15.2 million) in value. Monaco has extradited criminals, mainly to Russia, and has largely completed negotiations with the United States on a seized asset sharing agreement.

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

The Securities Regulatory Commissions of Monaco and France signed a memorandum of understanding (MOU) on March 8, 2002, on the sharing of information between the two bodies. The Government of Monaco considers this MOU an important tool to combat financial crime, particularly money laundering. SICCFIN has signed information exchange agreements with thirteen counterparts and is a member of the Egmont Group.

Monaco was admitted to the Council of Europe on October 4, 2004. In 2002, Monaco became a member of the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). 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.

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 applying its AML reporting, customer identification, and record keeping requirements to all trustees, as well as Monegasque gaming houses. Monaco should also eliminate the ability to open and maintain accounts using an alias, and banks should include their cashiers in customer identification responsibilities. Monaco should become a party to the UN Convention against Corruption. 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.

Montenegro

The Republic of Montenegro declared independence from the State Union of Serbia and Montenegro on June 3, 2006. Montenegro is located on the Balkan Peninsula in southeastern Europe, bordering the Adriatic Sea to the west, and sharing land borders with Croatia, Bosnia and Herzegoviva, Serbia and Albania. Montenegro has a population of about 630,000.

Montenegro continues to have a significant black market for smuggled goods. Illegal proceeds are generated from drug trafficking, official corruption, tax evasion, organized crime and other types of financial crimes. Proceeds from illegal activities are being heavily invested in all forms of real estate. The construction and renovation of commercial buildings such as offices, apartments, high-end retail businesses as well as personal residences is evident in the capital city Podgorica as well as other major

cities. Investment by foreign individuals and businesses in expensive real estate along the Montenegro coast has raised prices and generated concerns about the source of funds used for these investments.

Tax evasion, which is a predicate crime for money laundering, and trade-based money laundering in the form of over-and-under-invoicing, are common methods used to launder money. In Montenegro, the difficulty of convicting a suspect of money laundering without a conviction for the original criminal act and the unwillingness of the courts to accept circumstantial evidence to support money laundering or tax evasion charges is hampering law enforcement and prosecutors in following the movement and investment of illegal proceeds and effectively using the anti-money laundering laws.

In August 2002, the Central Bank of Montenegro (CBCG) issued a decree that requires banks and other financial institutions to report suspicious transactions, establish anti-money laundering control programs, and train their employees to detect money laundering. The CBCG dissolved all offshore banks for failure to re-register and reestablish themselves as regular banks. The Finance Ministry has not released complete information about the actual disposition of the 400 offshore entities whose names they turned over to CBCG. Currently, neither offshore entities, nor free trade zones, are authorized by Montenegro.

Money laundering was criminalized in 2002, and the Criminal Code was amended in June 2003 to enable the government to confiscate money and property involved in criminal activity. Additionally, according to the Criminal Code, business licenses of legal or natural persons may be revoked and business activities banned if the subject is found guilty of criminal activities, including narcotics trafficking or terrorist financing. In April 2004, Montenegro further amended its Criminal Procedure Code to bring it into conformity with the standards of the Council of Europe.

The Government of Montenegro (GOM) passed anti-money laundering legislation on September 24, 2003. The law obliges banks, post offices, state entities, casinos, lotteries and betting houses, insurance companies, jewelers, travel agencies, auto and boat dealers, and stock exchange entities to file currency transaction reports (CTRs) on all transactions exceeding 15,000 euros (approximately $19,000). Financial institutions are also obliged to report suspicious transactions, regardless of the amount of the transaction. All reporting by banking institutions is forwarded electronically to Montenegro's financial intelligence unit (FIU), called the Administration for the Prevention of Money Laundering, or APML. Failure to report, according to the law, could result in fines up to $26,000 as well as sentences of up to 12 years. Legislation in force since 2005 expanded Montenegro's money laundering law to include attorneys and exchange houses as obligated entities. A newly formed interagency working group is discussing and developing relevant amendments to the anti-money laundering legislation to bring it into conformity with the third EU Directive on Money Laundering.

Montenegro's FIU, the Administration for the Prevention of Money Laundering and Terrorist Finance (APML), is an independent agency which has the authority to collect, analyze and disseminate currency reports to the competent authorities for further action. The FIU became operational in November 2003 and began receiving reports of transactions in July 2004. However, APML has developed no guidelines regarding what should be considered a suspicious transaction.

The Montenegro FIU became an Egmont member in June 2005. It has executed a number of Memoranda of Understanding to exchange information with most established FIUs in the region, as well as with counterpart nonregional states, such as Russia and Ukraine. APML has also signed memoranda of cooperation with law enforcement bodies from the ministries of Justice and Customs, the tax authority and the Central Bank. However, the European Commission found that Montenegro must "substantially upgrade" its coordination and information exchange among these entities in order to effectively address money laundering issues.

In the first nine months of 2006, Montenegro's FIU received over 100,000 CTRs and 152 reports of suspicious transactions. Over 70,000 of the CTRs were filed by the stock exchange and nearly 30,000

were filed by banks. The FIU initiated the analysis of 106 transactions and referred 20 cases to other responsible government agencies for further action. The referrals resulted in 15 cases where subject accounts were blocked for 72 hours in order to permit further investigation of the transactions. In 2005, Montenegro blocked a total of $10.9 million. During the first eight months of 2006, this figure had increased to $23.4 million.

Montenegro can seize and forfeit assets. In September 2004, the Government of Montenegro seized over $1 million in undeclared currency in connection with the arrest of two Chinese nationals attempting to enter Montenegro. Further investigation revealed that these individuals had moved over $4 million in illicit funds through bank accounts in Montenegro. The two Chinese nationals' convictions were upheld on appeal, and on September 29, 2006 each was sentenced to one year in prison.

Montenegro is vulnerable to smuggling, particularly stolen cars, narcotics, cigarettes, and counterfeit goods. Customs and law enforcement authorities have expressed concern about trade-based money laundering. Customs is required to report cross-border movements of cash, checks, securities and precious metals and stones with values exceeding 15,000 euros.

Montenegro has criminalized the financing of terrorism and in March 2005 has subsequently adopted amendments to its laws on terrorism and terrorist financing in order to bring Montenegrin law into conformance with international standards. Responsibility for the detection and prevention of terrorist financing was transferred in 2004 from the CBCG to the FIU. The FIU circulates to banks and other financial institutions the names of suspected terrorists and terrorist organizations listed on the UNSCR 1267 Sanction Committee's consolidated list. Montenegro has identified a small number of terrorism financing cases. These cases, however, were not related to entities sanctioned by the UN Security Council.

Because of the demise of the State Union of Serbia and Montenegro, Serbia became the legacy member of the United Nations and the Council of Europe. Montenegro has obtained UN membership and its membership in the Council of Europe is pending. Because of these events, the GOM is now an observer in the Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) rather than a member. Montenegro is working on preparing an updated progress report on its achievements since MONEYVAL's first-round evaluation that was completed in 2003. This report will be presented to the plenary once Montenegro's membership is confirmed, which is expected to occur in early 2007. Likewise, the GOM is working toward ratification of the appropriate international conventions.

By the principle of state succession to the State Union of Serbia and Montenegro, Montenegro became a party to the 1988 UN Drug Convention, the UN International Convention on the Suppression of Financing of Terrorism, the UN Convention Against Transnational Organized Crime, and the UN Convention against Corruption on October 23, 2006.

The Government of Montenegro should strengthen its legislation to establish more robust asset seizure and forfeiture regimes, as well as upgrade its capacity to strengthen its criminal intelligence and investigative techniques. Montenegro should continue to ensure that sufficient resources are available for its FIU and law enforcement agencies to work together effectively and efficiently. The GOM should continue to participate in international fora that offer training and technical assistance for police, customs, and judiciary officials involved with combating money laundering and terrorist financing.

Morocco

Morocco is not a regional financial center, and the extent of the money laundering problem in the country is unknown. Nonetheless, according to a joint 2005 study by the United Nations Office on

Drugs and Crime (UNODC) and Morocco's Agency for Promotion of Economic and Social Development of the Northern Prefectures, Morocco remains an important producer and exporter of cannabis. The narcotics trade and the country's large informal economy are the primary catalysts of money laundering. In the past few years, the Kingdom has taken a series of steps to control the problem. A draft anti-money laundering (AML) bill was presented to the Parliament on November 20, 2006. Reportedly, passage of the AML law is expected to occur in 2007.

Remittances from abroad and cash-based transactions comprise Morocco's informal economic sector. There are unverified reports of trade-based money laundering, including bulk cash smuggling, under- and over-invoicing, and the purchase of smuggled goods; the cash-based cannabis sector is of particular concern. As in previous years, Morocco remains a principal producer of cannabis, with estimated revenues of over $13 billion annually. While some of the narcotics proceeds are laundered in Morocco, most proceeds are believed to be laundered in Europe.

Unregulated money exchanges remain a problem in Morocco and were a prime impetus for the pending Moroccan AML legislation. Although the legislation is intended to curb this practice, the country's current financial structure provides opportunities for unregulated cash transfers. The Moroccan financial sector consists of 16 banks, five government-owned specialized financial institutions, approximately 30 credit agencies, and 12 leasing companies. The monetary authorities in Morocco are the Ministry of Finance and the Central Bank, Bank Al Maghrib (CBM), which monitors and regulates the banking system. A separate Foreign Exchange Office regulates international transactions. There were no prosecutions for money laundering in Morocco in 2006. A key aspect of the pending AML legislation is the increase in responsibility for all entities, both public and private, to report suspect fund transfers, which will provide the legal basis to monitor and prosecute previously unregulated financial activity.

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, Moroccan security officials arrested over 50 suspects in August and September 2006 for their involvement in the Ansar Al Mahdi terrorist cell. At least two of the suspects 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. 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) that was inaugurated in Bahrain in November 2004. The creation of the MENAFATF is critical for pushing the region to improve the transparency and regulatory frameworks of its financial sectors.

Morocco is in the process of tightening anti-money laundering controls. Since 2003, Morocco has taken a series of steps to control money laundering. In December 2003, the CBM issued Memorandum

No. 36, in advance of the pending AML legislation, which 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 and the retention of suspicious activity reports, as well as mandating "know your customer" procedures. In June 2003, Morocco adopted a comprehensive counterterrorism bill. The 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 law brought Morocco into compliance with UNSCR 1373 requirements for the criminalization of the financing of terrorism. Other money laundering controls include legislation prohibiting anonymous bank accounts and foreign currency controls that require declarations to be filed when transporting currency across the border.

Morocco's anti-money laundering (AML) efforts will take a significant step forward with the implementation of long-awaited AML legislation, expected to occur in the first half of 2007. The legislation draws largely from recommendations made by the Financial Action Task Force (FATF). Once signed into law, the legislation reportedly will require the reporting of suspicious financial transactions by all responsible parties, 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.

Morocco should enact AML legislation that adheres to international standards, including the establishment of a centralized Financial Intelligence Unit (FIU). The AML legislation should provide the legal basis for the government to monitor, investigate, and prosecute all suspect financial activities. Police and customs authorities, in particular, should receive training on recognizing money laundering methodologies, including trade-based laundering and informal value transfer and underground remittance 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 comes from 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 the borders with Germany and Belgium, the Dutch authorities run special operations in the border areas to keep smuggling to a minimum. Reportedly, money laundering amounts to 18.5 million euros (approximately $24.4 million) 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 the 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 wide application of the money laundering offenses by stating that the public prosecutor does not need to prove the exact origin of laundered proceeds and that the general criminal origin as well as the knowledge of the perpetrator may be deducted 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 $59,000), while "liable acts" of money laundering (of 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 $59,000). Habitual money laundering may be punished with a maximum imprisonment of six years and a maximum fine of 45,000 euros (approximately $59,000), 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 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 15,000 euros (approximately $19,700), as well as any less substantial transaction that appears unusual, a broader standard than "suspicious" transactions, to the Office for Disclosure of Unusual Transactions (MOT), the Netherlands' financial intelligence unit (FIU). In December 2001, the reporting requirements were expanded to include trust companies, financing companies, and commercial dealers of high-value goods. In June 2003, notaries, lawyers, real estate agents/intermediaries, accountants, business economic consultants, independent legal advisers, trust companies and other providers of trust related services, and tax advisors were added. Reporting entities that fail to file reports with the MOT may be fined 11,250 euros (approximately $14,775), or be imprisoned up to two years. Under the Services Identification Act, all those that are subject to reporting obligations must identify their clients, including the identity of ultimate beneficial owners, either at the time of the transaction or prior to the transaction, before providing financial services.

In 2004, an evaluation of the anti-money laundering reporting system, commissioned by the Minister of Justice, was published. In response to the report the GON enacted a number of measures to enhance the effectiveness of the existing system. In November 2005, the Board of Procurators General issued a National Directive on money laundering crime that included an obligation to conduct a financial investigation in every serious crime case, guidelines for determining when to prosecute for money laundering and technical explanations of money laundering offenses, case law, and the use of financial intelligence. A new set of indicators, which determine when an unusual transaction must be filed, also entered into force in November 2005. These new indicators represent a partial shift from a rule-based to a risk-based system and are aimed at reducing the administrative costs of reporting unusual transactions for the reporting institutions without limiting the preventive nature of the reporting system. The Dutch parliament has also approved amendments to the Services Identification Act and Disclosure Act that expand supervision authority and introduce punitive damages. The revised legislation, which became effective on May 1, 2006, incorporates a terrorist financing indicator in the reporting system.

Financial institutions are also required by law to maintain records necessary to reconstruct financial transactions for at least 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. Financial institutions and all other 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. Furthermore, current legislation requires Customs authorities to report unusual transactions to the MOT; however, the Netherlands does not currently have a currency declaration requirement for incoming travelers. Under the 2004 Dutch European Union (EU) Presidency, the EU reached agreement on a cash courier regulation, which implements the Financial Action Task Force (FATF) Special Recommendation Nine on terrorist financing. The implementation is expected to occur in the Netherlands mid-2007.

The Money Transfer and Exchange Offices Act, which was 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 has to be identified and all transactions totaling more than 2,000 euros (approximately $2,630) must be reported to the MOT.

The Central Bank of the Netherlands, which merged with the Pension and Insurance Chamber in April 2004, and the Financial Markets Authority, as the supervisors of the Dutch financial sector, regularly exchanges information nationally and internationally. Sharing of information by Dutch supervisors does not require formal agreements or memoranda of understanding (MOUs).

The financial intelligence unit (FIU) for the Netherlands is a hybrid administrative-law enforcement unit that in 2006 combined the traditional FIU, Meldpunt Onjebruikelijke Transacties (MOT), 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 the BLOM merged, the resulting entity was integrated within the National Police (KLPD). The new unit is called the FIU-the Netherlands. This new FIU structure provides an administrative function that receives, analyzes, and disseminates the unusual and currency transaction reports filed by banks and financial institutions. It also provides a police function that serves as a point of contact for law enforcement. It forwards suspicious transaction reports with preliminary investigative information to the Police Investigation Service and to the FIU. This new organization responds to requests from foreign FIUs for financial and law enforcement information. Over the last five years, the MOT and the BLOM cooperated closely in responding to international requests for information, so this merger has not changed the nature of the Dutch reporting system. FIU-the Netherlands is part of the Egmont Group.

The MOT receives over 98 percent of unusual transaction reports electronically through its secure website. In 2004, the MOT received 174,835 unusual transaction reports, totaling over 3.2 billion euros (approximately $4 billion) and forwarded 41,003 to the BLOM and other police services as suspicious transactions for further investigation. In 2005, the MOT received 181,623 reports, totaling over 1.1 billion euros (approximately $1.4 billion), and forwarded 38,481to the BLOM and other police services. The average amount reported was 29,000 euros (approximately $36,500) in 2005, a decrease from the 79,000 euros (approximately $94,500) average reported in 2004. Reportedly, this significant decrease was due to a few large transactions in the previous year.

In order to facilitate the forwarding of suspicious transactions, the MOT and BLOM 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 the BLOM. On January 1, 2003, the MOT and BLOM formed a special unit (the MBA-unit) to work together to analyze data generated from the IST. Once the data is analyzed by the MBA-unit, it 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. MOT/BLOM provides the anti-money laundering division of Europol with suspicious transaction reports, and Europol applies the same analysis tools as BLOM.

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 the proceeds of a crime tracked to illegal activities. Property subject to confiscation as an instrumentality may consist of both moveable property and claims. Assets can be seized as a value-based confiscation. Asset seizure and confiscation legislation also provides for the seizure of additional assets controlled by a drug trafficker. Legislation defines property for the purpose of confiscation as "any object and any property right." Proceeds from narcotics asset seizures and forfeitures are deposited in the general fund of the Ministry of Finance. Dutch authorities have not identified any significant legal loopholes that allow drug traffickers to shield assets.

In order to promote the confiscation of criminal assets, the GON has instituted special court procedures. These procedures enable law enforcement to continue financial investigations in order 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, the Camden Asset Recovery Network (CARIN) was set up in The Hague in September 2004. BOOM played a leading role in the establishment of this informal international network of asset recovery specialists, whose aim is the exchange of information and expertise in the area of asset recovery.

Statistics provided by the Office of the Public Prosecutor show that the amount of assets seized in 2005 amounted to 11 million euros (approximately $14.5 million). 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 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 has designed a new centralized approach for large confiscation cases and a more flexible approach for handling smaller cases. Both took effect in 2006 and significantly increase 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 the Jihad and conspiracy with the aim of committing a serious terrorist crime separate 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" was passed in 1977 and 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 "Clearing-House" procedure. 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 MOT all transactions (actually carried out or intended) that involve persons, groups, and entities that have been linked, either domestically or internationally, with terrorism. Any terrorist crime will automatically qualify 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. The Dutch have taken steps to freeze the assets of individuals and groups included on the UNSCR 1267 Sanctions Committee's consolidated list. 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 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 identification of a target. 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 was automatically included in the list that is part of 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 Act on Terrorist Offenses took effect on August 10, 2004. The Act introduces Article 140A of the Criminal Code, which criminalizes participation in an organization when the intent is to commit acts of terrorism, 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. The GON is considering new legislation that would expand, among other things, investigative powers and the use of coercive measures in antiterrorist inquiries. In June 2004, the Dutch for the first time successfully convicted two individuals of terrorist activity allowing use of intelligence of the General Intelligence and Security Service (AIVD) as evidence. Nine individuals were convicted in March 2006 on charges of membership in a terrorist organization.

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 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 in the registers of 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 in order 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 replace the current initial screening of founders of private and public-limited partnerships and foundations with an ongoing screening system. The new system will be introduced in 2007 to improve Dutch efforts to fight fraud, money laundering, and terrorist financing.

Data about alternative remittance systems such as hawala or informal banking as a potential money laundering/terrorist financing source is still scarce. 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 will also initiate 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 and Third EU Money Laundering Directives. The Dutch have implemented some obligations resulting from these directives, such as effective supervision of money transfer offices, trust and service provider companies, and the incorporation of reporting on terrorist financing.

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 two agreements in the area of mutual legal assistance and extradition, stemming from the agreements that were concluded in 2003 between the EU and the United States. One of the amendments to the existing bilateral agreement is the exchange of information on bank accounts.

The MOT supervised the PHARE Project for the European Union (March 2002-December 2003). The PHARE Project was the European Commission's Anti-Money Laundering Project for Economic Reconstruction Assistance to Estonia, Latvia, Lithuania, Poland, the Czech Republic, Slovakia, Hungary, Slovenia, Romania, Bulgaria, Cyprus, and Malta. The purpose of the project was to provide support to Central and Eastern European countries in the development and/or improvement of anti-money laundering regulations. Although the PHARE project concluded in December 2003, the MOT has 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). In March 2006, the Dutch hosted a major international terrorist financing conference.

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 participates in the Caribbean Financial Action Task Force as a Cooperating and Supporting Nation. As a member of the Egmont Group, MOT 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, and the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime.

The Netherlands should continue with its plans for a screening system for private and public-limited partnerships, and implement requirements for all charities to register with a state or state-sanctioned body that is set up to perform screening. The GON should also devote more resources toward getting better data and a better understanding of alternate remittance systems in the Netherlands, and channel more investigative resources toward underground banks. The Netherlands should also continue to its plans to implement improved procedures for tracing informal bank systems, including prosecution procedures where appropriate, and improve coordination vis-à-vis the responsibilities of the various involved agencies.

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 islands have seven local commercial banks, four foreign commercial banks, 12 credit unions, six specialized credit institutions, one savings bank, four savings and credit funds, 15 consolidated international banks and 19 nonconsolidated international banks. There are 54 institutional investors operating in the Netherlands Antilles, including ten life insurance companies, 20 non-life insurance companies and 24 pension funds. There are also two life captive-insurance businesses, 15 non-life captive-insurance business and four professional re-insurers.

The Netherlands Antilles has a significant offshore financial sector with 229 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 2006, there were a total of 15,009 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 32 licensed internet gaming companies.

On February 1, 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 offence in the Netherlands Antilles. Legislation in 1993 and subsequent interpretations regarding the underlying crime establish that prosecutors do not need to prove that a suspected money launderer also committed an underlying crime in order to obtain a money laundering conviction. Thus, it is sufficient to establish that the money launderer knew, or should have known, of the money’s illegal origin. Suspicious transactions are required by law to be reported to the financial intelligence unit (FIU), the Meldpunt Ongebruikelijke Transacties (MOT NA).

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. The 2002 National Ordinance on Supervision of Fiduciary Business institutes the Supervisory Board to oversee the international financial sector. At the same time, the GONA imposed know-your-customer rules upon the sector. 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 under the obligation to report unusual transactions to the MOT NA. Each financial sector has its own reporting threshold amount. The GONA is currently amending its legislation to add new reporting entities, including lawyers, accountants, notaries, jewelers and real estate agents. It is expected that the legislation will be passed in 2007.

Through October 2006, 10,788 suspicious transaction reports totaling $1.3 billion were received by the MOT NA. Of these, 283 were reported to the relevant law enforcement authorities. The MOT NA currently has a staff of nine, and is engaged in increasing the effectiveness and efficiency of its reporting system. Significant progress has been reported in automating unusual 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 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 laws and regulations on bank supervision provide that international banks must have a physical presence and maintain records on the island. The Central Bank also supervises insurance companies, insurance brokers, mutual funds and administrators of these funds, all of which must be licensed by the Central Bank. As of 2003, supervision of the company service providers in the Netherlands Antilles was transferred to the Central bank.

The Central Bank updated its anti-money laundering guidelines in 2003. These guidelines are more closely focused on banks, insurance companies, pension funds, money transfer services, financial administrators, and company service providers and specifically include terrorism 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 shall report money of NAF 20,000 (approximately US$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 $142,000) and/or face one year in prison.

In 2000, the National Ordinance on Freezing, Seizing and Forfeiture of Assets Derived from Crime was enacted. The law allows the prosecutor to seize the proceeds of any crime proven in court.

Terrorist financing is not a crime in the Netherlands Antilles. However, in January 2002, the GONA enacted legislation 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) was signed between the Netherlands Antilles and the United States. As of the end of 2006, implementing legislation was pending the GONA parliament to allow this agreement to go into effect. The Mutual Legal Assistance Treaty between the Netherlands and the United States applies 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 also a member of the Caribbean Financial Action Task Force (CFATF), and as part of the Kingdom of the Netherlands, participates in the Financial Action Task Force (FATF). In 1999, the Netherlands extended application 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 ratify the Convention.

The Government of the Netherlands Antilles has demonstrated a commitment to combating money laundering. The Netherlands Antilles should continue its focus on increasing regulation and supervision of the offshore sector and free trade zones, as well as pursuing money laundering investigations and prosecutions. The GONA should criminalize the financing of terrorism and enact the necessary legislation to implement the UN International Convention for the Suppression of the Financing of Terrorism.

Nicaragua

Nicaragua is not a regional financial center. Nicaragua is not a major drug producing country, but 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 rule of law, judicial corruption, the politicization of the public prosecutor's office and insufficient funding for law enforcement institutions, makes Nicaragua's financial system an attractive target for narcotics-related money laundering. 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. However, this concern has not translated into an appreciable strengthening of Nicaragua's legal and institutional frameworks to effectively combat money laundering and the financing of terrorism.

Nicaragua's geographical position, with access to both the Atlantic and the Pacific Oceans and porous border crossings to its north and south, 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, trafficking of immigrants and the financing of terrorism.

While Nicaragua has pledged to fight the financing of terrorism, money laundering and other financial crimes, limited resources, corruption (especially 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. The current Prosecutor General and some Supreme Court justices advocate a narrow interpretation of money laundering law, claiming that, as written, Nicaraguan law only penalizes the laundering of proceeds of narcotics trafficking and not of other illegal activities. This position is believed to be politically motivated, as it would provide legal justification to overturn the conviction of former president Arnoldo Aleman for laundering the proceeds of corruption-related offenses. Regardless of this legally erroneous position, the Prosecutor General still refuses to prosecute narcotics offenders for money laundering despite ample evidence to support these types of cases. In the last 18 months, the National Prosecutor's Office has not prosecuted a single money laundering case, including those involving drug traffickers with large stashes of U.S. currency who have been arrested on Nicaraguan soil. This enforcement problem is exacerbated by the fact that the country does not have an operational FIU. All attempts to correct this deficiency have been stalled in the National Assembly, awaiting final resolution of Arnoldo Aleman's money laundering conviction.

A number of foreign institutions own significant shares of the Nicaraguan financial sector. In 2005, GE Consumer Finance, one of the largest financial service firms in the world, bought a 49.99 percent stake in Banco de America Central (BAC), which operates in several Central American countries, including Nicaragua. In October 2006, Citibank purchased a significant share of Grupo Financiero Uno's Central American operations, which include credit cards, commercial banking, insurance and

brokerage firms. The deal awaits regulatory approval. Banistmo, a Panamanian bank, operates in Nicaragua. Bancentro/Lafise, a financial institution covering all commercial banking and insurance services, maintains operations in El Salvador, Guatemala and Honduras. The entry into force on April 1, 2006, of the Central America/Dominican Republic Free Trade Agreement (CAFTA-DR) and increased pace of regional integration suggest growing involvement of Nicaraguan financial institutions with international partners and clients. Most large Nicaraguan banks already maintain correspondent relationships with Panamanian institutions.

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 regulations 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.

In 2005, the National Assembly reformed the law governing Nicaragua's general banks, nonbank financial institutions and financial groups, bringing it in line with Basel II international banking regulations. When enforced properly, the law will hold bank officials responsible for all of their institution's actions, including failure to report money laundering. Article 164 of the law calls for sanctions for 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.

In 1999, Nicaragua passed Law 285, which requires all financial institutions 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. 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 $10,000 or its equivalent in foreign currency. Law 285 is not, however, being used as an effective tool against money laundering crimes committed by organized crime groups. The National Prosecutor's and the Attorney General's legal positions on Law 285 differ significantly. The National Prosecutor, who also heads the CAF, has sought to limit the application of the money laundering law to drug crimes. The Attorney General has led President Bolanos's charge against public corruption, and has argued in and out of court that the money laundering law as written applies to public corruption and other nondrug crimes.

On paper, the CAF is composed 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 trained personnel, equipment and strategic goals. The CAF is headed by the National Prosecutor, who receives the reports from banks and decides whether to refer them to the Nicaraguan National Police (NNP) for further investigation. The Economics Crimes Unit within the NNP is in charge of investigating financial crimes, including money laundering and terrorist financing. The Nicaraguan Deputy Attorney General is critical of the inactivity and ineffectiveness of the CAF. He has claimed that of the suspicious activity reports received by the CAF from financial institutions, not a single criminal money laundering investigation—including those related to drug trafficking—has been initiated by the National Prosecutor.

Legislation that would improve Nicaragua's anti-money laundering regime has been stalled in the National Assembly for years. There are at least two pending bills: an amended drug and anti-money

laundering law which would better define the crime of money laundering, and a special bill to create a central FIU that would replace and enhance the functions of the CAF and establish more stringent reporting requirements.

Draft legislation to criminalize terrorist financing is under consideration by the National Assembly, without any sign of imminent passage. In spite of the lack of terrorist financing legislation, many elements of terrorist financing can theoretically be prosecuted under existing laws. Through five SIBIOF administrative decrees, Nicaragua also has the authority to identify, freeze and seize terrorist-related assets, but has not as yet identified any such active cases. However, Nicaragua has not yet established the financing of terrorism as a criminal offense, placing it in a position of noncompliance with international standards.

Reportedly, there are no hawala or other similar alternative remittance systems operating in Nicaragua, and Nicaragua 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. Over 300 micro-finance institutions exist in Nicaragua, serving over 300,000 clients, dominating the informal economy and managing a significant portion of the remittances. This sector has grown steadily at about 25 percent per year since 1999. While currently unregulated, a bill to bring this sector under the authority of the SIBOIF will be presented to the National Assembly in 2007.

Corruption within the judiciary is a serious problem: judges often let detained drug suspects go free after a short detention, a practice that puts drug traffickers back on the streets and thus increases the threat of money laundering. In a recent high profile case, judges released over $600,000 of funds from a suspected drug trafficker. From all indications, a number of judges may have been involved in the case and may have received payoffs. In another judicial scandal, two Mexican citizens believed to be involved in drug trafficking were acquitted, and over $300,000 in undeclared currency that Nicaraguan customs seized when they entered the country was returned to them. This case also involved a judge connected to the first drug-money scandal. Several judges have been exposed in the press for allegedly taking bribes to acquit drug traffickers at trials or to set aside their convictions on appeal. Other judges have been known to release drug defendants on bail for unsubstantiated medical reasons. Due to the rampant corruption in the Nicaraguan judiciary, the United States has cut off direct assistance to the Nicaraguan Supreme Court. U.S. anticorruption efforts have focused on creating a vetted Anti-Corruption Unit that would be housed within the NNP and include officials from the Attorney General's Office, with the aim of enhancing investigations and prosecutions of corruption, money laundering and related crimes.

In spite of corruption within the judicial branch, 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. Given the corrupt nature of 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 NNP to work with them. For example, in December 2005, the SIBOIF closed down a business named Agave Azul that was allegedly operating an illegal Ponzi scheme. Agave Azul opened for business in May 2005, and by December 2005, approximately $8 million in U.S. currency had been deposited in its accounts in at least two U.S. banks. The SIBOIF notified the National Prosecutor about the scheme in early August 2005; however, the National Prosecutor has hampered the investigation through failure to act. Efforts to freeze the business' bank accounts in the United States were unsuccessful due to the failure of the NNP to provide complete financial information, and the unwillingness of the National Prosecutor to seek U.S. Government cooperation. Despite these failures, the case demonstrates 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.

Nicaragua is a party to the 1988 United Nations Drug Convention, the UN International Convention on the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. On February 15, 2006, Nicaragua ratified the UN Convention against Corruption. Nicaragua 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). CFATF, which monitors its members' compliance with the international anti-money laundering and counterterrorist financing standards established by the Financial Action Task Force (FATF), has criticized Nicaragua for its failure to prosecute money laundering beyond drug-related offenses, criminalize terrorist financing or create an effective FIU. 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 Western Hemisphere that is not a member of the Egmont Group.

The Government of Nicaragua needs to enhance its limited efforts to combat financial crime by expanding the predicate crimes for money laundering beyond narcotics trafficking, criminalizing terrorist financing, allocating the necessary resources to develop an effective financial intelligence unit, and combating 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 counterterrorist financing standards and controls.

Nigeria

The Federal Republic of Nigeria is the most populous country in Africa and is West Africa's largest democracy. Although Nigeria is not an offshore financial center; its 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 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 economic conditions to strengthen their ability to perpetrate all manner of 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, identity theft, and advance fee fraud. 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 2005 and 2006.

In addition to narcotics-related money laundering, advance fee fraud is a lucrative financial crime that generates hundreds of millions of illicit dollars annually for criminals. 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. This type of fraud is referred to internationally as "Four-One-Nine" (419), a reference to the fraud section in Nigeria's criminal code. 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. Through the internet, businesses and individuals around the world have been, and continue to be, targeted by perpetrators of 419 scams. The EFCC has

tried to combat 419-related cyber crimes, but there have only been a few recorded successes as a result of their cyber crime initiatives.

In June 2001, the Financial Action Task Force (FATF) placed Nigeria on its list of noncooperative countries and territories (NCCT) in combating money laundering and in April 2002, the United States issued an advisory to inform banks and other financial institutions operating in the United States of serious deficiencies in the anti-money laundering regime of Nigeria and to warn U.S. banks to give "enhanced scrutiny" to all financial transactions emanating from Nigeria or going to, or through it. In December 2002, Nigeria enacted three pieces of legislation: an amendment to the 1995 Money Laundering Act that extends the scope of the law to cover the proceeds of all crimes; an amendment to the 1991 Banking and Other Financial Institutions (BOFI) Act that expands coverage of the law to stock brokerage firms and foreign currency exchange facilities, gives the Central Bank of Nigeria (CBN) greater power to deny bank licenses, and allows the CBN to freeze suspicious accounts; and the Economic and Financial Crimes Commission (Establishment) Act that establishes the Economic and Financial Crimes Commission (EFCC), that coordinates anti-money laundering investigations and 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 anti-money laundering regime. FATF recognized the progress Nigeria made in implementing AML policies, the establishment of a financial intelligence unit (FIU) and the progress on money laundering investigations, prosecution and convictions. As a result, Nigeria was removed from the NCCT but the FATF enhanced monitoring its efforts for compliance with international standards.

In April 2003, the EFCC was formally constituted, with the primary mandate to investigate and prosecute financial crimes. It has recovered or seized assets from various people guilty of fraud 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. In an effort to expedite the trial process, the Commission has been assigned two high court judges in Lagos and two in Abuja to hear all cases involving financial crimes.

In 2004, the National Assembly passed the Money Laundering (Prohibition) Act (2004), which applies to the proceeds of all financial crimes. It also covers stock brokerage firms and foreign currency exchange facilities, in addition to banks and financial institutions. 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. In November 2004, the EFCC reported that the great majority of Nigeria's banks were not in compliance with the new law, typically by not adhering to the due diligence provisions of the law and by neglecting to file suspicious transactions reports (STRs). The EFCC promised a new initiative to educate bank personnel and the general public about the provisions of the law before imposing sanctions for noncompliance. Nigeria has not yet detected a case of terrorist financing laundered through the banking system. The UNSCR 1267 Sanctions Committee's consolidated list is periodically distributed to Nigerian financial institutions.

Under the 2004 Money Laundering (Prohibition) Act and 1995 Foreign Exchange (Monitoring and Miscellaneous Provisions) Act, money laundering controls apply to nonbanking financial institutions. 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 such businesses as the Federal Ministry of Commerce may designate. To date, the oversight of compliance by the Ministry of Commerce has not been very rigorous or effective.

In 2004, the Economic and Financial Crimes Commission (Establishment) Act of 2002 was amended. The 2004 EFCC act 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 commission's primary mandate is to investigate and prosecute financial crimes, and in particular to coordinate anti-money laundering investigations and information sharing in Nigeria and internationally.

In 2005, the EFCC established the Nigerian Financial Intelligence Unit (NFIU). The NFIU draws its powers from the Money Laundering (Prohibition) Act of 2004 and the Economic and Financial Crimes Commission Act of 2004. It is the central agency for the collection, analysis and dissemination of information on money laundering and terrorism financing. All financial institutions and designated nonfinancial institutions are required by law to furnish the NFIU with details of their financial transactions. Provisions have been included to give the NFIU power to receive suspicious transaction reports made by financial institutions and nondesignated financial institutions, as well as to receive reports involving the transfer to or from a foreign country of funds or securities exceeding $10,000 in value.

The NFIU is a significant component of the EFCC. It complements the EFCC's directorate of investigations but does not carry out its own investigations. The NFIU fulfills a crucial role in receiving and analyzing STRs. As a result, banks have improved both their timeliness and quality in filing STRs reported to the NFIU. Under the EFCC Act, safe-harbor provisions are provided. 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 NFIU has access to records and databanks of all government and financial institutions, and it has entered into memorandums of understandings (MOUs) on information sharing with several other financial intelligence centers. The establishment of the NFIU was part of Nigeria's efforts towards the removal of Nigeria from the NCCT list.

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. Due to the recent creation of the EFCC, the enactment of new laws, and a successful public enlightenment campaign, crimes such as bank fraud and counterfeiting are being reported and prosecuted for the first time. 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. The Nigerian Police Force is incapable of handling financial crimes because of corruption and poor institutional capacity. Currently, the EFCC is the agency most capable of effectively investigating and prosecuting financial crimes, including money laundering and terrorist financing. The EFCC coordinates all other agencies in financial crimes investigations.

In 2005, the EFCC marked significant successes in combating financial crime. Two fraudsters in a Brazilian bank scam involving a total of $242 million in assets were successfully prosecuted and convicted for terms of 25 and 12 years in prison, respectively. Their assets were seized, and they were ordered to give $110 million in restitution to the bank. The EFCC also returned $4.481 million to an elderly woman swindled by a Nigerian 419 kingpin in 1995. The kingpin was arrested, prosecuted, convicted, and is serving his prison sentence. A former inspector general of police was arrested and prosecuted for financial crimes valued at over $13 million. His assets were seized and bank accounts frozen. He is currently serving a prison sentence and still faces 92 charges of money laundering and official corruption. Currently, two sitting state governors are the subject of money laundering investigations. The EFCC, working with the FBI, also has an active case involving a group of money brokers using banks in the United States to launder money. The money laundering legislation of 2004

has given the EFCC the authority to investigate and prosecute such cases. The EFCC also has the authority to prevent the use of charitable and nonprofit entities as laundering vehicles, though no such case has yet been reported. There were 23 money laundering convictions in 2005 and 96 convictions through October 2006. The trial court process has improved after several experienced judges were assigned specifically to handle EFCC cases; this has motivated EFCC officials to bring more cases to court. Since its establishment the EFCC has reportedly seized assets worth $5 billion.

Depending on the nature of the case, the tracing, seizing, and freezing of assets may be done by the NDLEA, NPF, or the ICPC, in addition to the EFCC. The proceeds from seizures and forfeitures are remitted to the federal government, and a portion of the recovered sums is used to provide restitution to the victims of the criminal acts. 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. There were no significant narcotics related assets seizures in 2006.

For cases that are investigated by the EFCC, the seizure of property is governed by the EFCC (Establishment) Act of 2004. Section 20 of the act provides for the forfeiture of assets and properties to the federal government after the accused has been convicted of money laundering, including foreign assets acquired as a result of such crime. The properties subject to forfeiture are set forth in Section 24. They include any real or personal property that represents the gross receipts a person obtains directly as a result of the violation of the act or which is traceable to such gross receipts. They also include any property that represents the proceeds of an offense under the laws of a foreign country within whose jurisdiction such offense or activity would be punishable for a term exceeding one year. Section 25 states that all means of conveyance, including aircraft, vehicles, or vessels that are used or intended to be used to transport or in any manner to facilitate the transportation, sale, receipt, possession or concealment of economic or financial crimes would be punishable. Section 26 provides for circumstances under which property subject to forfeiture may be seized. Under the NDLEA act, farms on which illicit crops are cultivated can be destroyed. The banking community is cooperating with law enforcement to trace funds and seize or freeze bank accounts. It should be noted, however, that forfeiture is currently possible only under the criminal law. There is no comparable law governing civil forfeiture, but a committee has been set up by the EFCC to draft such legislation.

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 ranks 146 out of 163 countries in Transparency International's 2006 Corruption Perception 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. Nigeria has been instrumental in the establishment of a permanent secretariat for the Intergovernmental Task Force against Money Laundering in West Africa (GIABA). Nigeria has also ratified the African Union Convention on Preventing and Combating Corruption, which was adopted in Mozambique in July 2003.

The Government of Nigeria has done a better job in preventing and pursuing money laundering both within and outside the country in 2006. It should continue to engage with the FATF and other relevant international organizations to identify and eliminate remaining anti-money laundering deficiencies. Nigeria should continue to pursue their anticorruption program and support both the ICPC and EFCC in their mandates to investigate and prosecute corrupt government officials and individuals, while at the same time maintaining the independence of those entities, and prevent political encroachment. The supervision of banking and nonbanking financial institutions should be further strengthened and moved from the Ministry of Commerce. Nigeria should continue towards implementation of a

comprehensive anti-money laundering 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.

Pakistan

Pakistan is not considered a regional or offshore financial center; however, financial crimes related to narcotics trafficking, terrorism, smuggling, tax evasion and corruption are significant problems. Pakistan is a major drug-transit country. As a result of tighter controls in the financial sector, smuggling, trade-based money laundering, hawala, and physical cross-border cash transfers are the common methods used to launder money and finance terrorism in Pakistan. Pakistani criminal networks play a central role in the transshipment of narcotics and smuggled goods from Afghanistan to international markets. Pakistan has very little control of the border area, which allows the flow of smuggled goods to the Federally Administered Tribal Areas (FATA) and Balochistan. Goods such as foodstuffs, electronics, building materials, and other products that are primarily exported from Dubai to Karachi are falsely documented as destined for Afghanistan under the "Afghan Transit Trade Agreement," which allows goods to pass through Pakistan to Afghanistan exempt from Pakistani duties or tariffs. Through smuggling, corruption, avoidance of taxes, as well as barter deals for narcotics, many of the goods destined for Afghanistan find their way to the Pakistani black market. The proliferation of counterfeit goods and intellectual property rights violations generate substantial illicit proceeds that are laundered. A group of private, unregulated charities has also emerged as a major source of illicit funds for international terrorist networks. Another issue is the use of madrassas as training grounds for terrorists. The lack of control of madrassas, similar to the lack of control of Islamic charities, allows terrorist organizations to receive financial support under the guise of support of Islamic education.

Money laundering and terrorist financing are often accomplished in Pakistan via the alternative remittance system called hundi or hawala. This system is also widely used by the Pakistani people for informal banking and legitimate remittance purposes. Free trade zones do operate in Pakistan. The government established its first Export Processing Zone (EPZ) in Karachi in 1989 and has subsequently created additional EPZs in the Sindh and Balochistan provinces. Although no evidence has emerged of EPZs being used in money laundering, over-or under-invoicing is common in the region and could be used by entities operating out of these zones. Fraudulent invoicing is typical in hundi/hawala countervaluation schemes.

Pakistan has adopted measures to strengthen its financial regulations and enhance the reporting requirements for the banking sector, in order to reduce its susceptibility to money laundering and terrorism financing. For example, financial institutions must report within three days any funds or transactions they believe are proceeds of criminal activity. However, this is largely not observed by financial institutions because. Pakistan has not yet formally established a Financial Intelligence Unit (FIU) to which such reports of suspicious transactions can be filed. Additionally, there is no safe harbor provision for financial institutions to protect them from civil and criminal liability for filing such reports.

Pakistan has had a comprehensive anti-money laundering law under consideration by its parliament since 2005 although such legislation has not yet been enacted. As a result, the offense of money laundering cannot be prosecuted in Pakistan. Several law enforcement agencies have responsibility to enforce laws against financial crimes. The National Accountability Bureau (NAB), the Anti-Narcotics Force (ANF), the Federal Investigative Agency (FIA), and the Customs authorities all oversee Pakistan's law enforcement efforts. The major laws in these areas include: The Anti-Terrorism Act of 1997, which defines the crime of terrorist finance and establishes jurisdiction and punishments; the National Accountability Ordinance of 1999, which requires financial institutions to report corruption