Slovak Republic

Slovakia is not an important regional financial center. The geographic, economic, and legal conditions that shape the money laundering environment in Slovakia are typical of those in other Central European transition economies. Slovakia's location along the major lines of communication connecting Western, Eastern, and Southeastern Europe makes it a transit country for smuggling and trafficking in narcotics, mineral oils, and people. Organized crime activity and the opportunities to use gray market channels also lead to a favorable money laundering environment. Financial crimes such as fraud, tax evasion, embezzlement, and illegal business activity have been quite problematic for Slovak authorities.

In response to these problems, Slovakia has gradually strengthened the financial provisions of its criminal and civil codes through a series of amendments since 2000, which have resulted in an increased number of money laundering prosecutions. In 2006 a new Confiscation Law came into effect, strengthening the government's ability to seize assets gained through criminal activity. However, international monitors have suggested that the new law still contains significant loopholes. Despite a slight decline in staff resources, Slovakia's financial intelligence unit (FIU) and regional financial police have continued to increase filings, inspections, and the number of cases forwarded for prosecution.

Slovakia's original anti-money laundering legislation, Act No. 249/1994 (later amended by Act No. 58/1996) came into effect in 1994. Article 252 of the Slovak Criminal Code, Legalization of Proceeds from Criminal Activity, came into force at the same time. These measures criminalize money laundering for all serious crimes, and impose customer identification, record keeping, and suspicious transaction reporting requirements on banks. A money laundering conviction does not require a conviction for the predicate offense, and a predicate offense does not have to occur in Slovakia to be considered as such. The failure of a covered entity to report a suspicious transaction and "tipping off" are criminal offenses.

As a result of amendments made to the Slovak Civil Code in 2001, all banks in Slovakia were ordered to stop offering anonymous accounts. All existing owners of anonymous accounts were required to disclose their identity to the bank and to close the anonymous account by December 31, 2003. Owners of accounts that were not closed may withdraw money for an additional three-year non-interest-bearing grace period. However, funds remaining after January 1, 2007 will be confiscated and deposited in a fund for the administration of the Ministry of Finance, where they will be available for collection by the account holder for another five years. As of January 1, 2007, bearer passbook accounts will cease to exist.

Act No. 367/2000, On Protection against the Legalization of Proceeds from Criminal Activities, which came into force in January 2001, replaces the standard for suspicious transactions with an expanded definition of unusual business activity. According to this modified definition, an unusual business activity is any transaction that could result in the legalization of income, the source of which is suspected to be criminal. Such transactions include the attempted disposal of income or property with the knowledge or suspicion that it was acquired through criminal activity in Slovakia or a third country. Designated transactions also include the acquisition, possession, or use of real estate, moveable property, securities, money, or any other property with monetary value, for the purpose of concealing or disguising its ownership. However, the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) sent a team to perform a third-round mutual evaluation in May 2005; the resulting September 2006 Mutual Evaluation Report (MER) called for guidelines for each sector, noting that some sectors, such as gaming, do not have an understanding of what "unusual" is for that sector. The National Bank of Slovakia (NBS) or the Financial Market Authority (FMA), in addition to the Financial Police, have supervisory authority over the various financial institutions.

Act No. 367/2000 also expands the list of entities subject to reporting requirements to include foreign bank subsidiaries, the Slovak Export-Import Bank, nonbank financial institutions such as casinos, post offices, brokers, stock exchanges, commodity exchanges, securities markets, asset management companies, insurance companies, real estate companies, tax advisors, auditors, credit unions, leasing firms, auctioneers, foreign exchange houses, and pawnshops, all of which have been particularly susceptible to money laundering. The 2005 MONEYVAL MER stated that there was generally no reporting on the part of the designated nonfinancial business and professions (DNFBP), and that casinos and exchange houses had not reported at all. The Slovakian FIU estimated that out of approximately 100,000 obliged entities, only the banks and insurance companies have reported regularly, and the securities sector has produced a small number of reports. It is unclear whether the reporting obligations are understood by all the covered entities. Non profit organizations are generally exempt from reporting requirements.

As recommended in 2001 by a previous MONEYVAL (then called PC-R-EV) team in its second-round evaluation of Slovakia, the Government of Slovakia (GOS) amended Act No. 367/2000 in order to address shortcomings of the original legislation, and in order to comply with European Directive 2001/97/EC. As a result, Slovakian legislation is now in full harmony with the Second European Union (EU) Directive. The FATF's 2002-3 Annual Report stated that the amended legislation provided a "basically sound preventive legal structure." However, the recent MONEYVAL MER noted that there was no apparent national strategy and an absence of leadership in the overall national fight against money laundering and terrorist financing.

Amendments to Act No. 367/2000 in 2002 further extend reporting requirements to: antique, art, and collectible brokers; dealers in precious metals or stones, or other high-value goods; legal advisors; consultants; securities dealers; foundations; financial managers and consultants; and accounting services. Covered persons are required to identify all customers, including legal entities, if they find that the customers prepared or conducted transactions deemed to be suspicious, or if a sum or related sums exceeding approximately $19,000 within a 12-month period is involved. Insurance sellers must identify all clients whose premium exceeds approximately $1,200 in a year or whose one-time premium exceeds approximately $3,200. Casinos are obligated to identify all customers. Transactions may be delayed by the covered entities up to 48 hours, with another 24-hour extension allowed if authorized by the Financial Police. If the suspicion turns out to be unfounded, the state assumes the burden of compensation for losses stemming from the delay.

As a result of these modifications, money laundering convictions under Article 252 of the Criminal Code have increased gradually in recent years, with 33 confirmed cases between 2002-2005. Detailed statistics on money laundering convictions are not available, but, according to the financial police, auto theft is the most commonly prosecuted money laundering offense. There were no autonomous cases of money laundering convictions, since the FIU and regional financial police tend to forward for prosecution money laundering cases that are tied with broader organized crime activities. Corporate liability for money laundering is still inapplicable in Slovakia.

Slovak law is less than effective regarding the beneficial ownership of legal persons. The 2005 MONEYVAL MER stated that "Slovakian law does not require adequate transparency concerning beneficial ownership and control of legal persons." The law does not mandate identification on the Commercial Register for beneficial owners of a company purchasing or holding shares in another registered company, and information is unavailable for foreign companies registered in Slovakia. According to the MER, corporate liability is inapplicable under Slovakian law. There is no broad requirement to give any special attention to business relationships or transactions with legal or actual persons from countries not applying, or insufficiently applying, the FATF recommendations.

Spravodasjaká Jednotka Financnej Policie, was established on November 1, 1996, as a law enforcement style financial intelligence unit within the Police. Under a 2005 police reorganization, the

FIU, which had been a department within the Financial Police, was downgraded to one of eight divisions of the Bureau of Organized Crime. As a result, it is no longer headed at the director level, and has seen its numbers of staff decrease. The MONEYVAL team questioned the degree of autonomy and operational independence of the FIU since the change.

The FIU, or the Office to Fight Organized Crime (OFOC), focuses on all forms of organized crime, including narcotics, money laundering, human trafficking, and prostitution. The OFOC has four regional units of financial police, each responsible for a different part of Slovakia (Bratislava, Eastern Slovakia, Western Slovakia, and Central Slovakia), and four substantive units: the unusual business transactions unit, the obliged entities supervision unit, the unit for international cooperation and the unit for property checks. The FIU has jurisdictional responsibility over money laundering violations, receives and evaluates suspicious transaction reports (STRs), and collects additional information to establish the suspicion of money laundering. If justified, the unit forwards the case to one of the regional financial police units. All supervisory authorities must inform the FIU of any violation immediately upon discovery. Once enough information has been obtained to warrant suspicion that a criminal offense has occurred, the FIU takes appropriate measures, including asking a financial institution or bank to delay business or a financial transaction for 48 hours; however, the decision to delay transactions comes at the discretion of the financial institution and authorities acknowledge that transactions are rarely delayed. The FIU can also submit the case to the state prosecutor's office for investigation and prosecution. The MONEYVAL team found that the FIU's powers and duties were not clearly defined in legislation and not made distinct from other police powers and duties.

In 2005, the FIU received 1,273 reports alleging unusual financial transactions worth $341 million. It submitted 16 proposals for criminal prosecution (including six from previous years) with a value of $612 million and 341 proposals for tax prosecution (including 137 from previous years). In addition, the Financial Police regional units submitted 159 proposals for criminal prosecutions. In 2005, the OFOC conducted or started 97 on-site inspections of "obliged persons" and levied penalties in 36 cases with a total value of $143,000. Most criminal prosecution cases involved credit fraud. Most tax prosecution and on-site inspections uncovered abuse of Slovakia's value added tax system by local business owners.

Through the first ten months of 2006, the FIU received 1,158 reports with a total value of $315,000. Eight of these cases were submitted for prosecution, plus two outstanding cases from 2005. Financial Police regional units have submitted a further 177 cases for prosecution. A growing number of these cases involve organized groups transferring funds from neighboring countries (primarily Ukraine and Hungary) to Slovakia. The OFOC has carried out 68 on-site inspections during this timeframe, resulting in fines with a total value of $45,000.

The OFOC also has a supervisory role. Under section 10 of the AML law, the FIU has supervisory duty over the implementation of AML measures in financial institutions, and to this end, inspects these institutions. It also has sole supervisory authority over designated nonfinancial covered entities. The FIU has six officers in this unit, exercising supervisory responsibility over 100,000 institutions.

The Public Prosecutor Service is independent from executive power and supervises criminal prosecution measures performed by police and investigators. According to the MONEYVAL team, there is some cooperation and coordination taking place at the working level, but overall, this is a weakness in Slovakia's AML regime. The team also concluded that law enforcement is empowered, but needs more training, as well as policy and practical guidance, to ensure proactive financial investigations as well as to generate more cases and obtain convictions and confiscation orders.

In 2003, a law amending and supplementing the Criminal Procedure Code and Criminal Code entered into force. The amendment strengthens the competencies of law enforcement by granting investigators the authority to conduct sting operations and introduces provisions regarding corporate criminal liability. In addition, crown witnesses (a criminal who voluntarily opts to cooperate with law

enforcement bodies) are now protected by the law and can be granted immunity or receive a shortened sentence. This rule does not apply to those that organized or instigated the crime. To clarify ambiguities related to *inter alia* seizure and confiscation of proceeds, Slovakia amended both the Criminal Procedure Code and the Criminal Code in late 2005. The new law provides for mandatory forfeiture of proceeds of crime. It does not, however, allow for forfeiture from third party beneficiaries, and there are some concerns about the legal structure of the asset freezing and seizure regime to ensure that all indirect proceeds may be liable for confiscation. Shortly after the law entered into force on January 1, 2006, police officers involved with criminal investigations, as well as prosecutors and judges, were trained in substantive provisions of the new laws. The new laws also provides for specific sentencing guidelines for crimes, including 2-20 years for legalization of proceeds from criminal activity, and 2-8 years for not reporting unusual business transactions by obliged persons. No criminal prosecutions under the new law have been completed as of yet, though several have been forwarded by the FIU this year.

The Public Prosecutor Service also provides orders for the seizure of accounts within the pre-trial proceedings stage, and can order the use of information technology for enhanced investigations under Criminal Procedure Code Articles 79c,88 and 88e. There is also a Special Prosecutor Office and a Special Court, established by Act 258/2003 and which began operations on September 1, 2004. Act 258/2003 amends the Criminal Procedure Code to give this new Special Prosecutor jurisdiction over public officials, but also over the general public, for corruption; establishing, plotting, and supporting criminal and terrorist groups; extremely serious criminal offenses including those committed with a terrorist group; and economic criminal offense in excess of a designated threshold. Some money laundering cases have met these parameters and have been adjudicated by the Special Prosecutor's Office.

On June 23, 2005, Parliament approved the Law on Proving the Origin of Property, which came into force on September 1, 2005. According to the law, an undocumented increase in property exceeding an amount 200 times the minimum monthly wage would be scrutinized and could be considered illegal. Anyone who has suspicions that property that may have been acquired illegally may report it to the police. The police are then obliged to investigate the allegations, ultimately reporting to the Office of the Attorney General if findings are conclusive. The Attorney General's Office may then order the property to be confiscated. Despite its approval, the new law was still controversial, and its implementation was frozen by the Constitutional Courts on October 6, 2005. The Constitutional Court has not yet taken a final decision on this law.

Slovakia has responded to the problem of the financing of terrorism by amending its money laundering law with Act No. 445/2002, which criminalizes terrorist financing and obliges covered entities to report transactions possibly linked to terrorist financing. However, the reporting obligation with respect to terrorist financing is not sufficiently clear in the law. In addition, covered institutions have not received any guidance and no reports involving terrorist financing have been filed. The Criminal Code provides for an offense covering someone who "supports" a terrorist group. Authorities have acknowledged the possibility of proceeding for the aiding and abetting an offense of terrorism or the establishment of a terrorist group, but there is no jurisprudence on these points. The MONEYVAL team advised the authorities that the criminalization of terrorist financing solely on aiding and abetting is not in line with the standards set forth in the methodology. The MER also stated that the provisions are not wide enough to clearly criminalize collections of funds: with intention to carry out terrorist acts (whether they are used or not), for any activities undertaken by terrorist organizations, and with unlawful intent to be used by an individual terrorist.

All competent authorities in the Slovak Republic have full power to freeze or confiscate terrorist assets consistent with UNSCR 1373. According to Act No. 367/2000 and its later amendments, financial institutions are required to report to the regional financial police when they freeze or identify suspected terrorist-linked assets. The Government of Slovakia (GOS) has agreed to freeze

immediately all accounts owned by entities listed on the UNSCR 1267 Sanctions Committee's, the EU's consolidated lists, and those provided by the United States. The lists, however, are not distributed, but posted online. Obliged institutions have the responsibility to look at the names on the website and report if they have a match to any names on the list. Guidance and communication with the financial intermediaries and DNFBP community is weak. No terrorist finance-related accounts have been frozen or seized in Slovakia, but were a terrorism-related account to be identified, the financial police could hold any related financial transaction for up to 48 hours, and then gather evidence to freeze the account and seize any assets.

The GOS is a party to all 12 of the UN conventions and protocols against terrorism. However, as reported in its 2004 self-assessment questionnaire on anti-money laundering efforts for the Council of Europe (COE), Slovakia is still not fully compliant with the Financial Action Task Force's (FATF's) Special Recommendations on Terrorist Financing. The COE's Committee of Experts gave Slovakia a rating of "partial compliance" in 2004 with regard to Special Recommendation I (Implementation of UNSCR 1373) and Special Recommendation VII (enhanced scrutiny of transfers lacking originator information).

In late 2005, following its official release, Slovak authorities started to prepare for implementation of the Third EU Money Laundering Directive. After consultations with the Ministry of Finance, the Ministry of Interior, and the National Bank of Slovakia, the FIU has been tasked with drafting new legislation to comply with the Third Directive. The new legislation would also grant the FIU broader authority to work directly with prosecutors, tax authorities, and the regular police.

In 2002, the GOS ratified the UN International Convention for the Suppression of the Financing of Terrorism. The provisions of the Convention have been incorporated into amendments of the Bank Act, Penal Code, and Act No. 367/2000 and in March 2003, Slovakia elected to fully incorporate into its laws several optional terms of the convention. The FIU is a member of the Egmont Group and has signed memoranda of understanding (MOUs) with the FIUs of Slovenia, Monaco, Ukraine, Australia, Belgium, Poland, and the Czech Republic. The GOS also hopes to sign MOUs with Albania and Taiwan in 2006. Slovakia's FIU is the responsible authority for international exchange of information regarding money laundering under the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime.

Slovakia is a party to the European Convention on Mutual Legal Assistance in Criminal Matters, the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, the 1988 UN Drug Convention, and the UN Convention against Transnational Organized Crime. In June 2006, it also ratified the UN Convention against Corruption. Slovakia became a member of the Organization for Economic Cooperation and Development (OECD) in December 2000, thereby expanding its opportunities for multilateral engagement.

Slovakia is a member of the Group of States Against Corruption (GRECO), a platform of the Council of Europe to fight against corruption. GRECO carried out its Second Evaluation Round in early 2006, based on 17 recommendations made by GRECO in 2004. In its report issued in May 2006, GRECO concluded that Slovakia had implemented satisfactorily or dealt with in a satisfactory manner just under half of the 17 recommendations made by GRECO in 2004. GRECO evaluators were particularly concerned with the lack of mechanisms to fight corruption in the public sphere. Slovakia is a member of the Council of Europe and since 1997 has actively participated in the MONEYVAL Committee.

The Government of Slovakia (GOS) should continue to improve its anti-money laundering regime. Continued implementation of the provisions of Slovakia's anti-money laundering legislation will give the Slovak financial system greater protection by helping it prevent and detect money laundering in all financial sectors. Authorities should ensure that property and proceeds are equivalent in Article 252 and that this definition is contained in the law to avoid confusion on this issue. Slovakia should also provide guidance to, and improve supervision of its nonfinancial sectors to ensure that reporting

requirements are followed. Slovakia should implement formal AML supervision for exchange houses. Slovakia should provide adequate resources to assure that its FIU, law enforcement, and prosecutorial agencies are adequately funded and trained to effectively perform their various responsibilities, and work to enhance cooperation and coordination among these agencies and other competent authorities. Although all supervisory authorities need more staff and training, the FIU in particular needs to increase the number of staff so that the staffing is commensurate with its supervisory role. Slovakia should also take steps to include in its legislative framework the FATF-prescribed definition and treatment of beneficial owners. Authorities should consider criminal, civil or administrative sanction for money laundering in relation to legal persons.

With regard to fighting terrorism financing, the GOS should hone its legal framework to clarify the reporting obligation with respect to terrorist financing and issue guidance to covered institutions. Authorities can also amend the Criminal Code to ensure that criminalization of terrorist financing parallels international standards, including widening the parameters to sanction criminally collections of funds: with intention to carry out terrorist acts (used or not), for any activities undertaken by terrorist organizations, and with unlawful intent to be used by an individual terrorist.

In addition, the GOS can make the lists produced and circulated by the UN and the U.S. more readily accessible to obliged institutions by distributing them to the institutions instead of posting them online. This would also serve to enhance communication and provide an opportunity to give guidance to covered institutions.

South Africa

South Africa's position as the major financial center in the region, its relatively sophisticated banking and financial sector, and its large cash-based market, all make it a very attractive target for transnational and domestic crime syndicates. Nigerian, Pakistani, and Indian drug traffickers, Chinese triads, Taiwanese groups, Lebanese trading syndicates, and the Russian mafia have all been identified as operating in South Africa, along with South African criminal groups. The fact that a high number of international crime groups operate in South Africa and that there are few reported money laundering prosecutions indicate that South Africa remains a money laundering jurisdiction of concern. Although the links between different types of crime have been observed throughout the region, money laundering is primarily related to the illicit narcotics trade. Other common types of crimes related to money laundering are: fraud, theft, corruption, currency speculation, illicit dealings in precious metals and diamonds, human trafficking, stolen cars, and smuggling. Most criminal organizations are also involved in legitimate business operations. There is a significant black market for smuggled goods.

South Africa is not an offshore financial center, nor does it have free trade zones. It does, however, operate Industrial Development Zones (IDZs). The South African revenue service monitors the customs control of these zones. Imports and exports that are involved in manufacturing or processing in the zone are duty-free, provided that the finished product is exported. South Africa maintains IDZs in Port Elizabeth, East London, Richards Bay, and Johannesburg International Airport.

The Proceeds of Crime Act (No. 76 of 1996) criminalizes money laundering for all serious crimes. This act was supplemented by the Prevention of Organized Crime Act (no. 121 of 1998), which confirms the criminal character of money laundering, mandates the reporting of suspicious transactions, and provides a "safe harbor" for good faith compliance. Violation of this act carries a fine of up to rand 100 million (approximately $16,700,000) or imprisonment for up to 30 years. Regulations require suspicious transaction reports to be sent to the South African financial intelligence unit (FIU), the Financial Intelligence Centre (FIC). Both of these Acts contain criminal and civil forfeiture provisions.

In 2005, the Protection of Constitutional Democracy Against Terrorist and Related Activities Act came into effect. The Act criminalizes terrorist activity and terrorist financing and gave the government investigative and asset seizure powers in cases of suspected terrorist activity. The Act is applicable to charitable and nonprofit organizations operating in South Africa. The Act requires financial institutions to report suspected terrorist activity to the FIC. The FIC distributes the list of individuals and entities included on the United Nations 1267 Sanctions Committee's consolidated list.

The FIC began operating in February 2003. The mandate of the FIC is to coordinate policy and efforts to counter money laundering activities. The FIC similarly acts as a centralized repository of information and statistics on money laundering. The FIC is a member of the Egmont Group of financial intelligence units. In addition to the FIC, South Africa has a Money Laundering Advisory Council (MLAC) to advise the Minister of Finance on policies and measures to combat money laundering.

The Financial Intelligence Centre Act (FICA) requires a wide range of financial institutions and businesses to identify customers, maintain records of transactions for at least five years, appoint compliance officers to train employees to comply with the law, and report transactions of a suspicious or unusual nature. Regulated businesses include companies and firms considered particularly vulnerable to money laundering activities, such as banks, life insurance companies, foreign exchange dealers, casinos, and real estate agents. If the FIC has reasonable grounds to suspect that a transaction involves the proceeds of criminal activities, it forwards this information to the investigative and prosecutorial authorities. If there is suspicion of terrorist financing, that information is to be forwarded to the National Intelligence Service. There are no bank secrecy laws in effect that prevent the disclosure of ownership information to bank supervisors and law enforcement authorities. However, the lack of actual cases prosecuted indicates problems in reporting process, analysis, investigations, and/or commitment.

From March 2005 through March 2006, the FIC received 19,793 suspicious transaction reports (STRs), an increase of 25 percent from the previous year's 15,757 STRs. The FIC reports that this increase is due to the development and distribution of its batch-reporting tool and not related to an increase in financial institutions detecting suspicious transactions. Precise information is not available on how many of these STRs led to criminal investigations. However, the number of financial crime and terrorist finance investigations, prosecutions, and convictions is believed to be extremely low. In addition, the quality and consistency of the STRs remains uneven. This is problematic for a country which has vast experience in implementing international banking standards. The FIC and South Africa's banks struggle to provide effective and comprehensive training programs relating to STR reporting and there has been no evidence of an increase in the quality of suspicious transaction reports. This calls into question the political will of the South African government towards implementing an effective and transparent AML/CFT regime

Many banks state that the reporting requirements hamper their efforts to attract new customers. For example, if the customer has never traveled outside the country, they may not have supporting documentation (no driver's license or passport) to properly satisfy the due diligence laws. Also, retroactive due diligence requirements mean those account holders who do not present identifying documents in person risk having their accounts frozen. These requirements were fully implemented in September 2006, after which date transactions with accounts owned by still-unidentified persons were blocked. Reporting requirements were specifically waived for brokers assisting clients with a one-time amnesty offer according to the Exchange Control and Amnesty and Amendment of Taxation Laws of 2003.

Because of the cash-driven nature of the South African economy, alternative remittance systems that bypass the formal financial sector exist, used largely by the strong local Islamic community. Hawala networks in South Africa have direct ties to South Asia and the Middle East. Currently, there is no

legal obligation requiring alternative remittance systems to report cash transactions within the country. The South African Revenue Service (SARS) requires large cash amounts to be declared only at entry and exit points. Smuggling and border enforcement are major problems in South Africa.

The Financial Action Task Force (FATF) conducted a mutual evaluation of South Africa in 2003 and made several recommendations regarding controls on cross-border currency movement, thresholds, and amendments to the Exchange Control Act. While legislation has been adopted in response to the recommendations, full implementation has yet to take place.

South Africa has cooperated with the United States in exchanging information related to money laundering and terrorist financing. The two nations have a mutual legal assistance treaty and a bilateral extradition treaty. In June 2003, South Africa became the first African nation to be admitted into the Financial Action Task Force (FATF), and it held the FATF Presidency for the period June 2005-June 2006. South Africa is also an active member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body.

South Africa 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.

The South African Government should implement FATF Special Recommendation Nine and establish control over cross-border currency movement. It should regulate and investigate the country's alternative remittance systems. South Africa should increase steps to bolster border enforcement and should examine forms of trade-based money laundering and informal value transfer systems. It should fully implement the new law (Protection of Constitutional Democracy against Terrorist and Related Activities Act) against terrorist activity and terrorist financing. South Africa should publish the annual number of money laundering and terrorist financing investigations, prosecutions, and convictions.

Spain

Spain is not a European financial center. Spain plays a significant role in money laundering as a key point of entry and European base for the proceeds of Colombian narcotics trafficking organizations. Drug proceeds from other regions enter Spain as well, particularly proceeds from hashish trafficking and smuggling entering from Morocco and heroin money entering from Turkey.

Tax evasion in internal markets and smuggling of goods along the coastline also continue to be sources of illicit funds in Spain. Reportedly, Spanish authorities believe that tax evasion in cell phone and property industries is currently the most serious financial crime. The smuggling of electronics and tobacco from Gibraltar remains an ongoing issue. Airline personnel traveling between Spain and Latin America smuggle out bulk cash. Additional money laundering methodologies found in Spain include Colombian companies purchasing goods in Asia and sell them legally at drug cartel-run stores in Europe. Credit card balances are paid in Spanish banks for charges made in Latin America, and money deposited in Spanish banks is withdrawn in Colombia through ATM networks

An unknown percentage of the proceeds from drug-trafficking is invested in Spanish real estate, particularly in the booming coastal areas in the south and east of the country. Twenty-five percent of the 500 euro notes in use in Europe are in circulation in Spain. Reportedly, this is directly linked to the purchase of real estate to launder money. There are no known currency transactions of significance involving large amounts of U.S. currency and/or direct narcotics proceeds from U.S. sales.

In September 2006, Spanish police arrested eight people of Spanish and Colombian nationality for drug trafficking and money laundering. Government of Spain (GOS) officials estimate that the individuals may have laundered more than 13.5 million euro (approximately 17.8 million dollars). The

investigation began at the end of 2003 after a money laundering organization was dismantled when a vessel carrying 412 kilos of cocaine was intercepted in Togo.

In May 2006, 21 people were arrested and accused of being members of an international money laundering and drug-trafficking gang. Police seized 193 kilos of cocaine, weapons, money, and luxury vehicles imported from Germany and then sold in Spain to launder the proceeds. It is estimated that the criminal organization had laundered a total of 360 million euro (approximately 475 million dollars) since 2000. The arrested members are also implicated in other offenses such as corruption of minors, forgery, and fraud.

Although little of the money laundered in Spain is believed to be used for terrorist financing, money from the extortion of businesses in the Basque region is moved through the financial system and used to finance the Basque terrorist group. ETA informal nonbank outlets (such as "Locutorios"), make small international transfers for the immigrant community, and continue to be used to move money in and out of Spain. Spanish regulators also note the presence of hawala networks in the Islamic community.

Spain is not considered to be an offshore financial center, and does not operate any Free Trade Zones. Spanish law states that an entity can perform banking activity if its registered office, administration, and management reside within Spanish territory. Spanish law does not prohibit financial institutions from entering into banking relationships with shell banks. Financial institutions have no requirement to determine whether a respondent financial institution in a foreign country allows accounts used by shell banks. The GOS has no accurate estimate of the numbers of offshore banks, offshore international business companies, exempt companies, or shell companies. Spanish law does not recognize trusts, including those created in foreign countries. Offshore casinos and internet gaming sites are forbidden. However, online casinos often run from servers located outside of Spanish territory. GOS politicians have been critical of Gibraltar's role in this regard. Regulation can only occur through mutual judicial assistance or international agreements.

Money laundering was criminalized by Article 301 of the Penal Code. The criminalization of money laundering was added to the penal code in 1988 when laundering the proceeds from narcotics trafficking was made a criminal offense. The law was expanded in 1995 to cover all serious crimes that required a prison sentence greater than three years. Amendments to the code on November 25, 2003, which took effect on October 1, 2004, made all forms of money laundering financial crimes; any property, of any value, can form the basis for a money laundering offence, and a conviction or a prosecution for a predicate offense is not necessary to prosecute or obtain a conviction for money laundering. The penal code can also apply to individuals in financial firms if their institutions have been used for financial crimes. An amendment to the penal code in 1991 made such persons culpable for both fraudulent acts and negligence connected with money laundering. Spanish authorities can also prosecute money laundering from a predicate offense in another country, if the offense would be illegal in Spain.

Law 19/2003 regulating the movements of capital and foreign transactions implements the European Union (EU) Money Laundering Directive. The law obligates financial institutions to make monthly reports on large transactions. Banks are required to report all international transfers greater than 30,000 euros (approximately $39,600). The law also requires the declaration and reporting of internal transfers of funds greater than 80,500 euros (approximately $106,300). Individuals traveling internationally are required to report the importation or exportation of currency greater than 6,000 euros (approximately $7,900). Foreign exchange and money remittance entities must report on transactions above 3,000 euro (approximately $3,960). Reporting on transactions exceeding 30,000 euro from or with persons in countries or territories considered to be tax havens is also required. Law 19/2003 allows the seizure of up to 100 percent of the currency if illegal activity under financial crimes ordinances can be proven. Spanish authorities claim they have seen a drop in cash couriers

since the law's enactment in July 2003. For cases where the money cannot be connected to criminal activity, and has not been declared, the authorities may seize the money until the origin of the funds is proven.

The financial sector is required to identify customers, keep records of transactions, and report suspicious financial transactions. Spanish banks are required by law to maintain fiscal information for five years and mercantile records for six years.

Money laundering controls apply to most entities active in the financial system, including banks, mutual savings associations, credit companies, insurance companies, financial advisers, brokerage and securities firms, postal services, currency exchange outlets, casinos, and individuals and unofficial financial institutions exchanging or transmitting money. The 2003 amendments add lawyers and notaries as covered entities. Previously, notaries and lawyers were required to report suspicious cases, but now they are considered part of the financial system that is under the supervision of appropriate regulators. As of April 2005, most categories of designated nonfinancial businesses and professions (DNFBP) are subject to the same core obligations as the financial sector. The list of DNFBPs includes casinos, realty agents, dealers in precious metals and stones, as well as in antiques and art, legal advisors, accountants and auditors.

Article 3.2 of Law 19/1993 mandates that reporting entities should examine and commit to writing the results of an examination of any transaction, irrespective of amount, which by its nature may be linked to laundering of proceeds. Law 12/2003 reaffirms the obligation of reporting suspicious activities. Reporting entities are required to report to suspicious individual transactions to the Financial Intelligence Unit, or FIU. Financial institutions also have an obligation to undertake systematic reporting of unusual transactions, including physical movements of cash, travelers' checks, and other bearer instruments/checks drawn on credit institutions above 30,000 euro (approximately $39,600). The reporting obligation applies to the laundering of proceeds of all illicit activity punishable by a minimum of three years imprisonment, including terrorism or terrorist financing. Non Bank Financial Institutions (NBFIs) such as insurers, investment services firms, collective investment schemes, pension fund managers, and others are subject to these requirements.

Article 4 of Law 19/1993 and Article 15 of RD 925/1995 protect financial institutions and their staff for breach of any restriction on disclosure of information when reporting suspicious transactions. Reporting units must also take appropriate steps to conceal the identity of employees or managers making suspicious transaction reports.

Law 19/1993 and RD 925/1995 established The Executive Service of the Commission for the Prevention of Money Laundering (SEPBLAC), to act as Spain's FIU. SEPBLAC has the primary responsibility for any investigation in money laundering cases and directly supervises the anti-money laundering procedures of banks and financial institutions. SEPBLAC is an interdepartmental body chaired by the Secretary for Economic Affairs, and all of the agencies involved in the prevention of money laundering participate. The representatives include the National Drug Plan Office, the Ministry of Economy, Federal Prosecutors (Fiscalia), Customs, Spanish National Police, Civil Guard, CNMV (equivalent to the SEC), Treasury, Bank of Spain, and the Director General of Insurance and Pension Funds.

SEPBLAC coordinates the fight against money laundering in Spain. Its primary mission is to receive, analyze and disseminate suspicious and unusual transaction reports from financial institutions and DNFBPs. SEPBLAC also has supervisory and inspection functions and is directly responsible for the supervision of a large number of regulated institutions. For this reason, SEPBLAC has memoranda of understanding with the Bank of Spain, the National Securities Market Commission, and the Director General of Insurance and Pension Funds, in order for these regulators to supervise their sectors.

In June 2006, the Financial Action Task Force (FATF) released the third-round mutual evaluation report (MER) for Spain. The evaluation team noted some areas where Spain is not in full compliance with the Forty Recommendations and Nine Special Recommendations. The FATF MER called the FIU's supervisory capabilities ineffective because of limited resources; it also expressed concern regarding SEPBLAC's independence from the Bank of Spain.

SEPBLAC has access to the records and databanks of other government entities, financial institutions, and has formal mechanisms in place to share information domestically and with other FIUs, including FINCEN. SEPBLAC has been an active member of the Egmont Group since 1995. SEPBLAC received 493 requests for information from other FIUs in 2005, and made 143 requests to Egmont members. SEPBLAC received 2,502 suspicious transaction reports (STRs) in 2005. Thirty-seven STRs were used to initiate investigations.

Any member of the Commission may request an investigation. However, the FATF MER noted some concerns about the effectiveness of SEPBLAC's investigations, stating that at certain stages of the investigative process, obtaining account files can be time-consuming. The National Police and Anticorruption Police informed the evaluation team that they receive too many reports, and the reports they do receive are not adequate to serve as the basis for an investigation. SEPBLAC delegates responsibility to two additional organizations. The first is a secretariat in the Treasury, located in the Ministry of Economy. Following investigation and a guilty verdict by a court, this regulating body carries out penalties. Sanctions can include closure, fines, account freezes, or seizures of assets. Law 19/2003 allows seizures of assets of third parties in criminal transactions, and a seizure of real estate in an amount equivalent to the illegal profit.

Under Spain's currency control system, individuals and companies must declare the amount, origin, and destination of incoming and outgoing funds. Cash smuggling reports are shared between host government agencies. Provisional measures and confiscation provisions apply to persons smuggling cash or monetary instruments that are related to money laundering or terrorist financing. Gold, precious metals, and precious stones are considered to be merchandise and are subject to customs legislation. Failing to file a declaration for such goods may constitute a case of smuggling and would fall under the responsibility of the customs authorities.

All legal charities are placed on a register maintained by the Ministry of Justice. Responsibility for policing registered charities lies with the Ministry of Public Administration. If the charity fails to comply with the requirements, sanctions or other criminal charges may be levied.

The Penal Code provides for two types of confiscation: generic (Article 127) and specific, for drug-trafficking offences (Article 374). Article 127 of the Penal Code allows for broad confiscation authorities by applying it to all crimes or summary offenses under the Code. The effects, instruments used to commit the offense, and the profits derived from the offence can all be confiscated. Article 127 also provides for the confiscation of property intended for use in the commission of any crime or offence. It also applies to property that is derived directly or indirectly from proceeds of crime, regardless of whether the property is held or owned by a criminal defendant or by a third party. Article 374 of the Penal Code calls for the confiscation of goods acquired through drug trafficking-related crimes, and of any profit obtained. This allows for the confiscation of instruments and effects used for illegal drug dealing, as well as the goods or proceeds obtained from the illicit traffic. Consequently, all assets held by a person convicted of drug trafficking may be confiscated if those assets are the result of unlawful conduct.

A judge may impose provisional measures concerning seizures from any type of offense by virtue of the code of criminal procedure. Effects may be seized and stored by the judicial authorities at the beginning of an investigation. The Fund of Seized Goods of Narcotics Traffickers receives seized assets. This agency was established under the National Drug Plan. The proceeds from the funds are divided, with equal amounts going to drug treatment programs and to a foundation that supports

officers fighting narcotics trafficking. The division of assets from seizures involving more than one country depends on the relationship with the country in question. EU working groups determine how to divide the proceeds for member countries. Outside of the EU, bilateral commissions are formed with countries that are members of Financial Action Task Force (FATF), FATF-like bodies, and the Egmont Group, to deal with the division of seized assets. With other countries, negotiations are conducted on an ad hoc basis.

The banking community cooperates with enforcement efforts to trace funds and seize/freeze bank accounts. The law is unclear as to whether or not civil forfeitures are allowed. The GOS enforces existing drug-related seizure and forfeiture laws. Spain has adequate police powers and resources to trace, seize, and freeze assets. Spain disseminates limited statistics on money laundering and terrorist financing investigations, prosecutions and convictions as well as on property frozen, seized and confiscated. As of mid 2005, 36,105,720 euro (approximately 47.6 million dollars) had been seized.

The FATF MER team noted some shortcomings in the areas of customer due diligence, beneficial ownership of legal persons, and bearer shares. Anonymous accounts and accounts in fictitious names are precluded by Spanish legislation. Bearer shares are permitted in Spain, although not as many as in the past. Spanish authorities have taken steps to neutralize them, since 1998 ensuring that mere possession cannot serve as proof of ownership. However, they still exist, and it appears that the authorities are learning more about legal persons using such shares. The MER team cited the requirements to determine the beneficial owner as "inadequate."

The FATF MER gives Spain a good overall review with regard to terrorist financing. Spain has long been engaged in fighting terrorist organizations, including ETA, GRAPO and more recently, al-Qaida. Spanish law enforcement entities have identified several methods of terrorist financing: donations to finance nonprofit organizations (including ETA and Islamic groups); establishment of publishing companies that print and distribute books or periodicals for the purposes of propaganda, which then serve as a means for depositing funds obtained through kidnapping or extortion; fraudulent tax and subvention collections; the establishment of "cultural associations" used to facilitate the opening of accounts and provide a cover for terrorist finance activity; and alternate remittance system transfers.

Spain complies with all EU regulations concerning the freezing of terrorist assets. Crimes of terrorism are defined in Article 571 of the Penal Code, and penalties are set forth in Articles 572 and 574. Sanctions range from ten to thirty years' imprisonment with longer terms if the terrorist actions were directed against government officials. On March 6, 2001, Spain's Council of Ministers adopted a decision requesting the implementation of UNSCR 1373 in the Spanish legal framework. EU Council Regulation (EC) 881/2002, which obliges covered countries such as Spain to execute UNSCR 1373, is implemented through EC No. 2580/of 27 December 2001. Terrorist financing issues are governed by a separate code of law and commission, the Commission of Vigilance of Terrorist Finance Activities (CVAFT). This commission was created under Law 12/2003 on the Prevention and Blocking of the Financing of Terrorism. In addition to the EU Council Regulations, Law 12/2003, when implemented, will allow the freezing of any type of financial flow so as to prevent the funds from being used to commit terrorist acts. Spanish authorities' ability to freeze accounts granted in the most recent law is more aggressive than that of most of their European counterparts. Though many laws are transposed from European Union (EU) directives, Law 12/2003 on the prevention and freezing of terrorist financing surpasses EU Council requirements. However, the implementing regulations have yet to be announced.

As with all of the European Union countries, the obligation to freeze assets under UNSCR 1267 has also been implemented through the Council. Spain regularly circulates to its financial institutions the list of individuals and entities that have been included on the UN 1267 Sanctions Committee consolidated list. There were six actions taken against individuals or entities in 2005 under 1267

and/or 1373, for a total value of 83.75 euro ($106). The Terrorist Finance Watchdog Commission is charged with issuing freezing orders.

Spain is a member of the FATF, and co-chairs the FATF Terrorist Finance Working Group. Spain is a participating and cooperating nation to the South American Financial Action Task Force (GAFISUD), and a cooperating and supporting nation to the Caribbean Financial Action Task Force (CFATF). Spain is a major provider of counterterrorism assistance. SEPBLAC is a member of the Egmont Group and currently chairs the Outreach Committee Working Group. Spain provides anti-money laundering and counterterrorist finance assistance, particularly to Spanish speaking countries in Latin America.

The GOS has signed criminal mutual legal assistance agreements with Argentina, Australia, Canada, Chile, the Dominican Republic, Mexico, Morocco, Uruguay, and the United States. Spain's Mutual Legal Assistance Treaty with the United States has been in effect since 1993, and provides for sharing of seized assets, provided the request is made to the Spanish court hearing the case, rather than administratively. Spain has also entered into bilateral agreements for cooperation and information exchange on money laundering issues with fourteen countries around the world, as well as with the United States. SEPBLAC has bilateral agreements for cooperation and information exchange on money laundering issues with twenty-one FIUs around the world.

Spain actively collaborates with Europol, supplying and exchanging information on terrorist groups. In 2006, U.S. law enforcement agencies also reported excellent cooperation with their Spanish counterparts.

Spain is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN Convention against Corruption, and the UN International Convention for the Suppression of the Financing of Terrorism. Spain adheres to all EC policy directives on crime, money laundering, and the financing of terrorism.

The scale of money laundering and the sophisticated methods used by criminals create a significant law enforcement problem in Spain. The Government of Spain (GOS) has passed and enacted legislation designed to help eliminate and prosecute financial crimes. In light of the findings of the 2006 FATF mutual evaluation, Spain should review its supervisory regime with a view toward maximizing the coordination of inspections as well as interagency cooperation . Spain should also review the resources available for industry supervision. The GOS should work to close potential loopholes that FATF identified, including those in the areas of customer due diligence, beneficial ownership of legal persons, and bearer shares. . Spain should also work to implement Law 12/2003, which will greatly enhance Spain's capabilities to combat terrorism financing. Spain should maintain and disseminate statistics on investigations, prosecutions and convictions, including the amounts and values of assets frozen or confiscated.

St. Kitts and Nevis

The Government of St. Kitts and Nevis (GOSKN) is a federation composed of two islands in the Eastern Caribbean. The federation is at major risk for corruption and money laundering, due to the high volume of narcotics trafficking activity and the presence of known traffickers on the islands. The offshore financial sectors of both islands are vulnerable to money laundering. An inadequately regulated economic citizenship program compounds the problem.

Each island has the authority to organize its own financial structure. As a Federation, there is offshore legislation governing both St. Kitts and Nevis. However, with most of the offshore financial activity concentrated in Nevis, it has developed its own offshore legislation independently. As of September 2006, Nevis has one offshore bank (a subsidiary of a domestic bank), 61 licensed insurance companies, 1,014 international trusts, 29 foundations and 54 corporate service providers. There are two types of international companies eligible for incorporation: international business companies

(IBCs) and limited liability companies (LLCs). Current figures indicate there are 12,773 IBCs and 3,732 LLCs registered in Nevis. Reports from 2006 indicate that St. Kitts' offshore sector consists of 1,019 exempt companies, 203 exempt foundations, four trust companies, two investment companies, 21 corporate service providers, and three licensed internet gaming companies that must incorporate as IBCs. According to reports from 2004-2005, St. Kitts also has four domestic banks, 120 credit unions, four domestic insurance companies, and two money remitters. There are no free trade zones in St. Kitts and Nevis.

The GOSKN licenses offshore banks and businesses. Bearer shares are permitted, provided that bearer share certificates are retained in the safe custody of persons or financial institutions authorized by the Minister of Finance as approved custodians. Authorized service providers serve as a company's first directors or trustees; this information is made public. Subsequent to incorporation or registration, the authorized persons transfer such duties to other persons. This information is restricted to only the regulator and authorized persons who have access to the information. Reportedly, extensive background checks on all proposed licensees are conducted by a third party on behalf of the GOSKN before a license is granted. Under the Nevis Offshore Banking Ordinance 1996, as amended in 2002, the Eastern Caribbean Central Bank (ECCB) is required to review all applications for licenses and report its recommendations to the Minister of Finance prior to consideration of the application. By law, all licensees are required to have a physical presence in St. Kitts and Nevis. All authorized persons are required to obtain proper documents on shareholders or beneficial owners before incorporating IBCs or other offshore companies.

The Proceeds of Crime Act (POCA) 2000 criminalizes money laundering for serious offenses and imposes penalties ranging from imprisonment to monetary fines. The POCA also overrides secrecy provisions that may have constituted obstacles to the access of administrative and judicial authorities to information with respect to account holders or beneficial owners. Other anti-money laundering measures include the Financial Services Commission Act 2000, the Nevis Offshore Banking (Amendment) 2000, the Anti-Money Laundering Regulations 2001, the Companies (Amendment) Act 2001, the Anti-Money Laundering (Amendment) Regulations 2001, the Nevis Business Corporation (Amendment) 2001, and the Nevis Offshore Banking (Amendment) 2001.

The ECCB has direct responsibility for regulating and supervising the offshore bank in Nevis, as it does for domestic banks in St. Kitts and Nevis, and for making recommendations regarding approval of offshore bank licenses. The St. Kitts and Nevis Financial Services Commission, with regulators on both islands, regulates nonbank financial institutions for anti-money laundering compliance. The GOSKN has issued regulations requiring financial institutions to identify their customers upon request, maintain a record of transactions for up to five years, report suspicious transactions, and establish anti-money laundering training programs. The Financial Services Commission has issued guidance notes on the prevention of money laundering, pursuant to the Anti-Money Laundering Regulations. The Commission is authorized to carry out anti-money laundering examinations. The St. Kitts and Nevis Gaming Board is responsible for ensuring compliance of casinos.

The Financial Intelligence Unit (FIU) Act No. 15 of 2000 authorized the creation of an FIU. The FIU began operations in 2001 and receives, analyzes and investigates suspicious activity reports (SARs) from reporting entities in both St. Kitts and Nevis. All financial institutions, including nonbank financial institutions, are required by law to report suspicious transactions. Anti-money laundering regulations and the FIU Act provide protection for reporting entities and its employees, officers, owners or representatives who forward SARs to the FIU. In 2006, the FIU received 50 SARs. Of these, 20 SARs were referred to law enforcement for appropriate action. There have been no reports of further action taken on these referrals. The Royal St. Kitts and Nevis Police Force is responsible for investigating financial crimes, but does not have adequate staff or training to effectively execute its mandate. The FIU has direct and indirect access to records of other government agencies through

memoranda of understanding (MOU). The FIU Act has provisions for sharing information, both domestically and with foreign counterparts and law enforcement agencies.

Under the POCA legitimate businesses can be seized by the FIU if proven to be connected to money laundering activities. The FIU can freeze an individual's bank account for a period not to exceed five days in the absence of a court order. The freeze orders obtained from the court at times ascribe an expiration of six months or more. The law only allows for criminal forfeiture; civil forfeiture is considered unconstitutional. The POCA provides for a forfeiture fund under the administration and control of the Financial Secretary in St. Kitts and the Permanent Secretary in the Ministry of Finance in Nevis. All monies and proceeds from the sale of property forfeited or confiscated are placed in the fund to be used for the purpose of anti-money laundering activities in both St. Kitts and Nevis.

The POCA limits and monitors the international transportation of currency and monetary instruments. Any person importing or exporting a value exceeding US$10,000 or its equivalent in Eastern Caribbean currency needs to declare it with Customs. In addition, the Customs Control and Management Act criminalizes cash smuggling. Customs and law enforcement share cash smuggling reports.

St. Kitts and Nevis enacted the Anti-Terrorism Act (ATA) No. 21, effective November 27, 2002. Sections 12 and 15 of the Act criminalize the financing of terrorism. Under the ATA, the FIU and Director of Public Prosecutions have the authority to identify, freeze, and/or forfeit assets related to terrorist financing. The ATA also implements various UN Conventions against terrorism. The GOSKN circulates to financial institutions the names of individuals and entities that have been included on the UN 1267 Sanctions Committee's lists. To date, no terrorist-related funds have been identified. The ATA does not provide the FIU with the authority to receive disclosures relating to potential financing of terrorism from reporting entities. The GOSKN has some existing controls that apply to alternative remittance systems, but has not undertaken initiatives that apply directly to the potential terrorist misuse of charitable and nonprofit entities.

A Mutual Legal Assistance Treaty (MLAT) between the GOSKN and the United States entered into force in early 2000, but cooperation over the last three years has been stalled by the GOSKN. St. Kitts and Nevis 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. St. Kitts and Nevis is a party to the UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. The GOSKN has signed, but not yet ratified, the Inter-American Convention against Terrorism, and has neither signed nor ratified the UN Convention against Corruption. The FIU became a member of the Egmont Group in 2004.

St. Kitts and Nevis should devote sufficient resources to effectively implement its anti-money laundering regime, giving particular attention to its offshore financial sector. St. Kitts and Nevis should determine the exact number of Internet gaming companies present on the islands and provide the necessary oversight of these entities. St. Kitts and Nevis should amend the Anti-Terrorism Act to provide the FIU with the authority to receive disclosures relating to potential financing of terrorism from reporting entities. Additionally, St. Kitts and Nevis should improve its cooperation with foreign counterparts, particularly the timely information sharing on money laundering and financial crime activity and the implementation of bilateral agreements. St. Kitts should become a party to the UN Convention against Corruption.

St. Lucia

St. Lucia has developed an offshore financial service center that increases the island's vulnerability to money laundering and other financial crimes. Transshipment of narcotics (cocaine and marijuana),

unregulated money remittance businesses, cash smuggling, and bank fraud, such as counterfeit U.S. checks and identity theft, are among the other primary vulnerabilities for money laundering in St. Lucia.

Currently, St. Lucia has four offshore banks, 1,912 international business companies (IBCs), seven private mutual funds, two public mutual funds, 43 international trusts, 24 international insurance companies, 24 trust companies, two money remitters, three mutual fund administrators, 13 registered agents and four registered trustees (service providers), and a total of 30 domestic financial institutions. Shell companies are not permitted. The Government of St. Lucia (GOSL) also has one free trade zone where investors may establish businesses and conduct trade and commerce within the free trade zone or between the free trade zone and foreign countries. There are no casinos or internet gaming sites in St. Lucia. Reportedly, the GOSL does not plan to consider the establishment of gaming enterprises.

In 1999, the GOSL enacted a comprehensive inventory of offshore legislation, consisting of the International Business Companies (IBC) Act, the Registered Agent and Trustee Licensing Act, the International Trusts Act, the International Insurance Act, the Mutual Funds Act and the International Banks Act. An IBC may be incorporated under the IBC Act. Only a person licensed under the Registered Agent and Trustee Licensing Act as a licensee may apply to the Registrar of IBCs to incorporate and register a company as an IBC. The registration process involves submission of the memorandum and articles of the company by the registered agent, payment of the prescribed fee, and the Registrar's determination of compliance with the requirements of the IBC Act. IBCs can be registered online through the GOSL's web page. IBCs intending to engage in banking, insurance or mutual fund business may not be registered without the approval of the Minister responsible for international financial services. An IBC may be struck off the register on the grounds of carrying on business against the public interest.

The GOSL established the Committee on Financial Services in 2001. The Committee, which meets monthly, is designed to safeguard St. Lucia's financial services sector. The Committee is composed of the Minister of Finance, the Attorney General, the Solicitor General, the Director of Public Prosecutions, the Director of Financial Services, the Registrar of Business Companies, the Commissioner of Police, the Deputy Permanent Secretary of the Ministry of Commerce, the police officer in charge of the Special Branch, the Comptroller of Inland Revenue and others. The GOSL announced in 2003 its intention to form an integrated regulatory unit to supervise the onshore and offshore financial institutions the GOSL currently regulates. As of October 31, 2006, administrative procedures were implemented, but the unit is not yet fully functional. The Eastern Caribbean Central Bank regulates St. Lucia's domestic banking sector.

The 1993 Proceeds of Crime Act criminalizes money laundering with respect to narcotics. The Proceeds of Crime Act also provides for a voluntary system of reporting account information to the police or prosecutor when such information may be relevant to an investigation or prosecution. Reporting individuals (bankers and other financial institutions) are protected by the law with respect to their cooperation with law enforcement entities. In addition, the Act requires financial institutions to retain information on new accounts and transactions for seven years. In September 2003, legislation was adopted that extends anti-money laundering compliance requirements to credit unions, money remitters and pawnbrokers, as well as strengthens criminal penalties for money laundering.

Many of the 1993 Proceeds of Crime Act provisions are superseded by the 1999 Money Laundering (Prevention) Act (MLPA), which criminalizes the laundering of proceeds with respect to 15 predicate offenses, including abduction, blackmail, counterfeiting, extortion, firearms and narcotics trafficking, forgery, corruption, fraud, prostitution, trafficking in persons, tax evasion, terrorism, gambling and robbery. The MLPA mandates suspicious transaction reporting requirements and imposes record keeping requirements. In addition, the MLPA imposes a duty on financial institutions to take reasonable measures to establish the identity of customers, and requires accounts to be maintained in

the true name of the holder. It also requires an institution to take reasonable measures to identify the underlying beneficial owner when an agent, trustee or nominee operates an account. These obligations apply to domestic and offshore financial institutions, including credit unions, trust companies, and insurance companies. In April 2000, the Financial Services Supervision Unit issued detailed guidance notes, entitled "Minimum Due Diligence Checks, to be conducted by Registered Agents and Trustees." Currently steps are being taken to implement legislation to regulate money remitters.

The Financial Intelligence Authority Act No. 17 of 2002 authorizes the establishment of St. Lucia's financial intelligence unit (FIU), which became operational in October 2003. Pursuant to legislation passed in September 2003, the Money Laundering (Prevention) Authority, which had previously been responsible for monitoring compliance with the anti-money laundering provisions of the MLPA, was merged with the FIU. The FIU is responsible for receiving, analyzing and disseminating suspicious transaction reports (STRs) from obligated financial institutions, and has regulatory authority to monitor compliance with anti-money laundering requirements. The FIU is also able to compel the production of information necessary to investigate possible offenses under the 1993 Proceeds of Crime Act and the MLPA. Failure to provide information to the FIU is a crime, punishable by a fine or up to ten years imprisonment. The Financial Intelligence Authority Act permits the sharing of information obtained by the FIU with foreign FIUs. The FIU has access to relevant records and databases of all St. Lucian government entities and financial institutions. However, no formal agreement exists for sharing information domestically and with other FIUs.

In 2006, the FIU received 27 STRs. There are no recorded cases of money laundering within St. Lucia's banking sector for 2006. However, there has been an increase in bank fraud, such as counterfeit U.S. checks and identity theft.

Customs laws criminalize cash smuggling, and customs officials are aware of cash courier problems. Cash smuggling reports are shared with the FIU, Police, Director of Public Prosecutions and the Attorney General.

Under current legislation, instruments of crime, such as conveyances, farms, and bank accounts, can be seized by the FIU. Substitute assets can also be seized. The legislation also applies to legitimate businesses if used to launder drug money, support terrorist activity, or are otherwise used in a crime. There is no legislation for civil forfeiture or sharing of seized narcotics assets. If the individual or business is not charged, then assets must be released within seven days. Approximately $100,000 of nonterrorist related assets were frozen in 2006.

The GOSL has not criminalized the financing of terrorism. However, St. Lucia circulates lists to financial institutions of terrorists and terrorist organizations on the UN 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O 13224. The Government of St. Lucia has the legislative power to freeze, seize and forfeit terrorist finance related assets. To date, no accounts associated with terrorists or terrorist entities have been found in St. Lucia. The GOSL has not taken any specific initiatives focused on the misuse of charitable and nonprofit entities.

The GOSL has been cooperative with the USG in financial crime investigations. In February 2000, St. Lucia and the United States brought into force a Mutual Legal Assistance Treaty. St. Lucia also has a Tax Information Exchange Agreement with the United States.

St. Lucia is a member of the Caribbean Financial Action Task Force (CFATF) and the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. The FIU is not yet a member of the Egmont Group. St. Lucia is a party to the 1988 UN Drug Convention and has signed, but has not yet ratified, the UN Convention against Transnational Organized Crime and the Inter-American Convention against Terrorism. The GOSL has not signed the

UN International Convention for the Suppression of the Financing of Terrorism or the UN Convention against Corruption.

The Government of St. Lucia should become a party to 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 order to meet international standards, St. Lucia should criminalize the financing of terrorism. The GOSL should continue to enhance and implement its money laundering legislation and programs, including adopting civil forfeiture legislation and ensuring that its FIU meets the Egmont Group membership requirements. The rapid expansion of the island's offshore financial services sector should be counterbalanced by efforts that increase transparency. The GOSL also needs to improve their record of investigating, prosecuting and sentencing money launderers and those involved in other financial crimes.

St. Vincent and the Grenadines

As a result of their status as a transit point for illicit narcotics and its growing offshore sector, St. Vincent and the Grenadines (SVG) are vulnerable to money laundering and other financial crimes. Money laundering is most often associated with the production and trafficking of marijuana in SVG, as well as the trafficking of other narcotics from South America. The illicit narcotics proceeds are laundered through various financial institutions, including banks (both domestic and offshore), money remitters, cash couriers and casinos. Over the past year, there has been an increase in fraud and the use of counterfeit instruments, such as tendering counterfeit checks or cash.

The domestic sector is comprised of two commercial banks, a development bank, two savings and loan banks, a building society, 16 insurance companies, 10 credit unions and two money remitters. The offshore sector includes 6 offshore banks; 7,655 international business corporations (IBCs), an increase of more than 1,000 IBCs since 2005; 16 offshore insurance companies; 39 mutual funds; 33 registered agents; and 126 international trusts. No physical presence is required for offshore financial institutions and businesses. Nominee directors are not mandatory except when an IBC is formed to carry out banking business. Bearer shares are permitted for IBCs but not for banks. There are no free trade zones in SVG. There are no offshore casinos, and no internet gaming licenses have been issued. The Government of St. Vincent and the Grenadines (GOSVG) eliminated its economic citizenship program in 2001.

The Eastern Caribbean Central Bank (ECCB) supervises SVG's domestic banks. The International Banks (Amendment) Act 2002 provides the ECCB with the authority to review and make recommendations regarding the approval of offshore bank licenses. The International Financial Services Authority (IFSA) regulates the international financial sector and oversees the process of licensing and supervision of the sector, which includes conducting on-site inspections to evaluate the financial soundness and anti-money laundering programs of offshore banks.

The International Banks (Amendment) Act of October 2000 provides the GOSVG with access to the name or title of a customer account and any other confidential information about the customer that is in the possession of a licensee. In 2002, the International Business Companies Amendment Act No. 26 of 2002 was enacted to immobilize and register bearer shares. The Exchange of Information Act No. 29 of 2002 authorizes and facilitates the exchange of information, particularly among regulatory bodies.

The Proceeds of Crime and Money Laundering (Prevention) Act 2001 criminalizes money laundering, and requires financial institutions and other regulated businesses to report suspicious transactions. Customers are required to complete a source of funds declaration for any cash transaction over $10,000 ECD (approximately $3,800). However, it is not mandatory to report other noncash transactions exceeding $10,000 ECD. The Proceeds of Crime (Money Laundering) Regulations were

published in January 2002 and establish mandatory record keeping rules and limited customer identification requirements. Financial institutions are required to maintain all records relating to transactions for a minimum of seven years.

The Financial Intelligence Unit Act No. 38 of 2001 (FIU Act) establishes the financial intelligence unit (FIU). Operational as of 2002, the FIU investigates and prosecutes money laundering cases. As of November 2006, the FIU had received 97 suspicious transaction reports (STRs) for the year and almost 600 STRs since its inception. The FIU is also the main body that supervises the compliance of financial and nonfinancial institutions with anti-money laundering and counterterrorist financing laws and regulations. The FIU conducts anti-money laundering and counterterrorist financing awareness training to educate these entities of the legal reporting requirements. Reporting entities are protected by law if fully cooperative with the FIU. There were five money laundering cases pending in 2005. Two of these cases resulted in convictions in 2006.

The FIU Act, as amended, permits the sharing of information at the investigative or intelligence stage, but the FIU does not have direct access to the records or databases of other government agencies. The FIU Act allows for the exchange of information with other FIUs. An updated extradition treaty and a Mutual Legal Assistance Treaty (MLAT) between the United States and the GOSVG entered into force in September 1999. The FIU executes the MLAT requests. In 2003, the GOSVG reintroduced a customs declaration form to be completed by incoming travelers. Incoming travelers are required to declare currency over $10,000 ECD (approximately $3,800).

Existing anti-money laundering legislation allows for the forfeiting of intangible and tangible property. Drug trafficking offenses may also be liable to forfeiture pursuant to the Drug (Prevention and Misuse) Act and the Criminal Code. There is no period of time during which the assets must be released. Frozen assets are confiscated by the FIU upon conviction of the defendant. Proceeds from asset seizures and forfeitures are placed by the FIU into the Confiscated Assets Fund established by the Proceeds of Crime and Money Laundering (Prevention) Act. Legitimate businesses can also be seized if used to launder drug money, support terrorist activity, or are otherwise used in a crime. At this time, only criminal forfeiture is permitted; however, a civil forfeiture bill is currently being debated. In 2006 the GOSVG froze or seized approximately 666,693 ECD (approximately $251,600) in assets. Of this amount, approximately 51,000 ECD ($19,200) worth of assets were forfeited.

The GOSVG enacted the United Nations Terrorism Measures Act in 2002. In July 2006, parliament enacted amendments to the Act and the FIU Act to ensure compliance with international standards and require financial institutions to report suspicious activity related to the financing of terrorism to the FIU. The GOSVG circulates lists of terrorists and terrorist entities to all financial institutions in SVG. To date, no accounts associated with terrorists have been found. The GOSVG has not undertaken any specific initiatives focused on the misuse of charitable and nonprofit entities.

The GOSVG 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 FIU became a member of the Egmont Group in 2003. The GOSVG is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. The GOSVG has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the Inter-American Convention against Terrorism. The GOSVG has not signed the UN Convention against Corruption.

The GOSVG has strengthened its anti-money laundering regime through legislation and the establishment of an effective FIU. The GOSVG should insist that the beneficial owners of IBCs are known and listed in a registry available to law enforcement; immobilize all bearer shares; and properly supervise and regulate all aspects of its offshore sector. The GOSVG should continue to provide training to its regulatory, law enforcement, and FIU personnel in money laundering operations and

investigations. The GOSVG should pass civil forfeiture legislation and consider the utility of special investigative techniques.

Switzerland

Switzerland is a major international financial center, with some 338 banks and a large number of nonbank financial intermediaries. Authorities suspect that Switzerland is vulnerable at the layering and integration stages of the money laundering process. Switzerland's central geographic location, relative political, social, and monetary stability, wide range and sophistication of available financial services, and long tradition of bank secrecy—first codified in 1934—are all factors that make Switzerland a major international financial center. These same factors also make Switzerland attractive to potential money launderers. However, Swiss authorities are aware of these issues and are sensitive to the importance of financial services to the Swiss economy. Total assets and liabilities in Swiss banking institutions were over 2.4 trillion Swiss francs ($1.8 trillion) in 2004, with foreigners accounting for over half of this figure. By comparison, Switzerland's GDP in 2004 was approximately $250 billion.

Reporting indicates that criminals attempt to launder proceeds in Switzerland from a wide range of illegal activities conducted worldwide, particularly financial crimes, narcotics trafficking, arms trafficking, organized crime, terrorism financing, and corruption. Although both Swiss and foreign individuals or entities conduct money laundering activities in Switzerland, narcotics-related money laundering operations are largely controlled by foreign narcotics trafficking organizations, often from the Balkans or Eastern Europe. Some of the money generated by Albanian narcotics trafficking rings in Switzerland has been funneled to armed Albanian extremists in the Balkans.

Swiss bank accounts also frequently figure in investigations of fraud and corruption of government officials and leaders, most often from foreign countries. Due to the large amount of foreign asset management within Switzerland, the likelihood of illicit funds being held in Switzerland is relatively high, despite measures taken to combat this phenomenon. Recent examples of public figures that have been the subject of money laundering allegations or investigations include a former President of Kyrgyzstan, a former Russian Minister of Atomic Energy, and the family of the Nigerian dictator Sani Abacha in connection with the funds (approximately$748 million) that Abacha had hidden in Swiss banks between 1993 and 1998. In June 2005, the former Swiss Ambassador to Luxembourg was sentenced to three and a half years in jail for money laundering and other crimes.

The Financial Action Task Force (FATF) conducted a mutual evaluation of Switzerland's anti-money laundering and counterterrorist financing regime in 2005. The mutual evaluation report (MER) concluded that Switzerland was at least partially compliant in most areas. However, the evaluators found Switzerland's anti-money laundering regime to be less than compliant with respect to correspondent banking and cash couriers.

Money laundering has been a criminal offense in Switzerland since 1998, when the Federal Act on the Prevention of Money Laundering in the Financial Sector (MLA) entered into effect. Swiss law, however, currently does not recognize certain types of criminal offenses as part of the eighty "serious crimes" that serve as predicate offenses for money laundering, including illegal trafficking in migrants, counterfeiting and pirating of products, smuggling, insider trading, and market manipulation. The adoption of anti-money laundering (AML) regulations planned for 2007 will make these crimes predicate offenses. Fiscal offenses do not constitute "serious crimes," so they are not considered to be predicate offenses.

Switzerland has significant AML legislation in place, subjecting banks and other financial intermediaries to strict know-your-customer (KYC) and reporting requirements, including the requirement to identify the beneficial owner of accounts. Negligence in this area is punishable under Swiss law. Switzerland has also implemented legislation for identifying, tracing, freezing, seizing, and

forfeiting narcotics-related assets. Legislation that aligns the Swiss supervisory arrangements with the Basel Committee's "Core Principles for Effective Banking Supervision" is contained in the Swiss Money Laundering Act.

Swiss money laundering laws and regulations apply to both banks and nonbank financial institutions. The Federal Banking Commission (FBC), the Federal Office of Private Insurance, and the Swiss Federal Gaming Board serve as the primary oversight authorities for a number of financial intermediaries, including banks, securities dealers, insurance institutions, and casinos. Other financial intermediaries are required to either come under the direct supervision of the Money Laundering Control Authority (MLCA) of the Federal Finance Department or join an accredited self-regulatory organization (SRO). SROs are nongovernmental self-regulating organizations authorized by the Swiss government to oversee implementation of AML measures by their members. SROs must be independent of the management of the intermediaries they supervise and must enforce compliance with due diligence obligations. Noncompliance can result in a fine or a revoked license. About 6,000 financial intermediaries are associated with SROs; the majority of these are financial management companies.

The Swiss Bankers Association (SBA) had employed customer due diligence (CDD) provisions as part of the industry standard in its Code of Conduct prior to any anti-money laundering legislation. The Code of Conduct was implemented by the SBA and enforced by the FBC, the supervisory authority over the banks. The FBC later implemented a "Policy on Prevention and Fight Against Money Laundering," establishing guidelines for the banking industry to employ in fighting money laundering. With the MLA, the Code of Conduct, CDD provisions and money laundering policy were extended to the entire financial sector. The Swiss Federal Banking Commission's AML regulations were revised in 2002 and became effective in 2003. These regulations, aimed at the banking and securities industries, codify a risk-based approach to suspicious transaction and client identification and install a global know-your-customer risk management program for all banks, including those with branches and subsidiaries abroad. In the case of higher-risk business relationships, additional investigation by the financial intermediary is required. The regulations require increased due diligence in the cases of politically exposed persons by ensuring that decisions to commence relationships with such persons be undertaken by at least one member of the senior executive body of a firm. All provisions apply to correspondent banking relationships as well. Swiss banks may not maintain business relationships with shell banks (banks with no physical presence at their place of incorporation), but there is no requirement that banks ensure that foreign clients do not authorize shell banks to access their accounts in Swiss banks.

The 2002 Banking Commission regulations mandate that all cross-border wire transfers must contain identifying details about the funds' remitters, though banks and other covered entities may omit such information for "legitimate reasons." The Federal Banking Commission has said that there are no plans at the moment to follow EU regulations aimed at registering names, addresses, and account numbers of those making even small money transfers between EU member states.

In July 2003, the government-sponsored Zimmerli Commission, tasked by the Department of Finance with examining reform of finance market regulators, presented 46 recommendations. Among the most far-reaching of these was the recommendation to merge the Federal Banking Commission and the Federal Office for Private Insurance-the institutions supervising the banking and insurance sectors-into a single, integrated financial market supervision body, to be called FINMA. In November 2004, the Cabinet instructed the Department of Finance to draft a parliamentary bill providing for the establishment of FINMA. Under the Cabinet's proposal, MLCA would also be included within FINMA. The draft bill is expected to be adopted by Parliament during the 2007 winter session, and enforced 12-18 months later, possibly by the end of 2008.

Switzerland's banking industry offers the same account services for both residents and nonresidents. Banks offer certain well-regulated offshore services, including permitting nonresidents to form offshore companies to conduct business, which can be used for tax reduction purposes. Pursuant to an agreement signed by the EU and Switzerland in 2004, EU residents have tax withheld on interest payments from savings accounts. This measure, enacted in concert with the EU's Savings Directive (2003/48/EC), was implemented on July 1, 2005, and may reduce the use of Swiss bank accounts by EU residents.

Swiss commercial law does not recognize any offshore mechanism per se and its provisions apply equally to residents and nonresidents. The stock company and the limited liability company are two standard forms of incorporation offered by Swiss commercial law. The financial intermediary is required to verify the identity of the beneficial owner of the stock company and must also be informed of any change regarding the beneficial owner. Bearer shares may be issued by stock companies but not by limited liability companies.

Switzerland has duty free zones. The customs authorities supervise the admission into and the removal of goods from customs warehouses. Warehoused goods may only undergo manipulations necessary for their maintenance, such as repacking, splitting, sorting, mixing, sampling and removal of the external packaging. Any further manipulation is subject to authorization. Goods may not be manufactured in the duty free zones. Swiss law has full force in the duty free zones; for example, export laws on strategic goods, war material, and medicinal products, as well as laws relating to anti-money laundering prohibitions, all apply. In view of the fact that customs authorities may and frequently do enter any customs warehouse area they choose, they believe they would be aware of the nature of any "value added" activity taking place in duty free zones.

Switzerland ranks fifth in the highly profitable artwork trading market, exporting $686 million worth of artwork worldwide in 2004. The Swiss market offers opportunities for organized crime to transfer stolen art or to use art to launder criminal funds. The United States is Switzerland's most important trading partner in this area, having purchased $253 million worth of art from Swiss sources in 2004. The 2003 Cultural Property Transfer Act, implemented in 2005, codifies in Swiss law elements of the 1970 United Nations Educational, Scientific, and Cultural Organization (UNESCO) Convention. This measure increases from five to thirty years the time period during which stolen pieces of art may be confiscated from those who purchased them in good faith. The law also allows police forces to search bonded warehouses and art galleries.

In January 2005, the Federal Council submitted a proposal for revisions based on the amended FATF Recommendations; the Federal Council revised this proposal in September. The October FATF mutual evaluation followed, and identified areas for improvement. In September 2006, the Federal Council instructed the Federal Department of Finance (FDF) to submit two papers addressing the FATF's proposal for improvements in the Swiss system; the proposal is designed to keep Swiss money laundering legislation current in the face of new challenges posed by international financial crime and to allow Swiss legislation to more thoroughly conform to international standards. The first paper, released at the end of 2006, addressed the proposal for revision of insider criminal law provisions on an accelerated basis. The second, due in mid-2007, will address other points from the FATF proposal. These points include: the creation of new predicate offenses for money laundering; the extension of the MLA to terrorist financing; the introduction of the obligation to report, if money laundering is suspected, that which prevents the establishment of a business relationship; and better legal protections against reprisals for financial intermediaries who report suspected money laundering. The paper also seeks to add some measures, including the introduction of an information system on cross-border transportation of currency valued in excess of CHF 25,000 ($20,500); the obligation to verify identification for financial intermediaries of representatives of legal entities; the obligation for the financial intermediary to establish the purpose and nature of the business relationship desired by the customer; and unlimited extension of the ban on tipping-off.

Established in 1998 by the MLA, the Money Laundering Reporting Office Switzerland (MROS) is Switzerland's financial intelligence unit (FIU), charged with receiving, processing and disseminating suspicious transaction reports (STRs). Although it is located in the Federal Office of Police, MROS is an administrative unit and does not have any investigative powers of its own, nor can it obtain additional information from reporting entities after receiving a STR. Under the MLA, MROS has five working days to process reports. In 2005, MROS received 729 reports involving approximately $536 million, an 11.2 per cent decrease in the number of reports compared to 2004. Whereas the decline in the number of reports in 2004 was mainly in the category of money transmitters, the decrease in 2005 was evident in nearly all categories of regulated entities. Unlike in the period 2002-2004, in 2005 the number of STRs filed by banks decreased.

Under the 2002 Efficiency Bill, the Swiss Attorney General is vested with the power to prosecute crimes addressed by Article 340bis of the Swiss Penal Code, which also covers money laundering offenses. In the past, the individual cantons (administrative components of the Swiss Confederation) were charged with investigating money laundering offenses. Additional legislation, effective January 1, 2002, increased the effectiveness of the prosecution of organized crime, money laundering, corruption, and other white-collar crime, by increasing the personnel and financing of the criminal police section of the federal police office. The law confers on the federal police and Attorney General's Office the authority to take over cases that have international dimensions, involve several cantons, or which deal with money laundering, organized crime, corruption, or white collar crime.

If financial institutions determine that assets were derived from criminal activity, the assets must be frozen immediately until a prosecutor decides on further action. Examining magistrates may order accounts to be frozen. Under Swiss law, suspect assets may be frozen for five days while a prosecutor investigates the suspicious activity. Since the MLA entered into force, CHF 423m ($348 million) have been frozen. Articles 58-60 of the Criminal Code outline measures relation to the confiscation of illicitly-obtained assets. Switzerland cooperates with the United States to trace and seize assets, and has shared a large amount of funds seized with the U.S. Government (USG) and other governments. The Government of Switzerland has worked closely with the USG on numerous money laundering cases.

Revisions to the Swiss Penal Code regarding terrorist financing entered into force on October 1, 2003. Article 260quinquies of the Penal Code provides for a maximum sentence of five years' imprisonment for terrorist financing. Article 100quater of the Penal Code, also added in 2003, extends criminal liability for terrorist financing to include companies. The FATF 2005 mutual evaluation team found Switzerland to be "largely compliant" with FATF Special Recommendation II regarding the criminalization of terrorist financing. The FATF team noted, however, that the Swiss Penal Code criminalizes the financing of an act of criminal violence but not the financing of an individual, independent of a particular act.

Since September 11, 2001, Swiss authorities have been alerting Swiss banks and nonbank financial intermediaries to check their records and accounts against lists of persons and entities with links to terrorism. The accounts of these individuals and entities are to be reported to the Ministry of Justice as suspicious transactions. Based on the "state security" clause of the Swiss Constitution, the authorities have ordered banks and other financial institutions to freeze the assets of suspected terrorists and terrorist organizations on the United Nations Security Council Resolution 1267 Sanctions Committee's consolidated list.

Along with the U.S. and UN lists, the Swiss Economic and Finance Ministries have drawn up their own list of approximately 44 individuals and entities connected with international terrorism or its financing. Swiss authorities have thus far blocked about 82 accounts totaling $25 million from individuals or companies linked to Usama Bin Laden and al-Qaida under relevant UN resolutions. Switzerland has also participated in joint task forces targeting the financing of al-Qaida cells. The

Swiss Attorney General also separately froze 41 accounts representing approximately $25 million on the grounds that they were related to terrorism financing, but the extent to which these funds overlap with the UN consolidated list is not clear.

MROS received 20 STRs relating to terrorist financing in 2005; the aggregate sum of money associated with these reports was 46 million Swiss francs (approximately$58 million). This represents an increase over the 11 reports related to terrorist financing submitted in 2004; these 11 reports involved a total of 900,000 Swiss francs (approximately $700,000). The higher number of reports in 2005 can be explained by the fact that several reports involved the same people or families and that one report alone involved 28.5 million Swiss francs (approximately $36 million). With the exception of 2 cases, MROS forwarded all the reports to the respective law enforcement agencies, which, in 6 of the 18 cases, did not investigate further.

Switzerland has ratified the Council of Europe's Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and is a party to the UN International Convention for the Suppression of the Financing of Terrorism. Switzerland ratified the 1988 UN Drug Convention on September 14, 2005, and the UN Convention against Transnational Organized Crime on October 27, 2006. Switzerland has signed, but not yet ratified, the UN Convention against Corruption and the International Convention for the Suppression of Acts of Nuclear Terrorism.

Swiss authorities cooperate with counterpart bodies from other countries. Switzerland has a mutual legal assistance treaty in place with the United States, and Swiss law allows authorities to furnish information to U.S. regulatory agencies, provided it is kept confidential and used for law enforcement purposes. Switzerland has been a member of FATF since its inception, and helped to shape the CDD and identification standards that the FATF adopted. Switzerland is also actively involved with the Basel Committee on Banking Supervision, establishing through it in 1988 the first international code of conduct for banks to prevent abuse of the industry by money laundering. MROS is a member of the Egmont Group. Swiss legislation permits "spontaneous transmittal," a process allowing the Swiss investigating magistrate to signal to foreign law enforcement authorities the existence of evidence in Switzerland. The Swiss used this provision in 2001 to signal Peru that they had uncovered accounts linked to former Peruvian presidential advisor Vladimiro Montesinos. However, on the principles of dual criminality, Switzerland has no legal basis to grant mutual legal assistance to foreign states where money laundering is based on fiscal offenses, because these do not serve as predicate offenses for money laundering in Switzerland.

The Government of Switzerland has stated that it hopes to correct the country's image as a haven for illicit banking services and works to improve its oversight on the banking and financial service sectors . The Swiss believe that their system of self-regulation, which incorporates a "culture of cooperation" between regulators and banks, equals or outperforms that of other countries. The primary orientation of the Swiss system is the aversion of risk at the account-opening phase, where due diligence and know-your-customer procedures address the issues, rather than relying on an early-warning system on all filed transactions. The Swiss Government believes that because of the due diligence approach the Swiss have taken, there are fewer STRs filed than in some other countries. At the same time, in 2005 MROS forwarded 69 percent of the STRs to law enforcement for further investigation.

While generally positive, Switzerland's recent FATF mutual evaluation report nonetheless identified weaknesses in the Swiss anti-money laundering and counterterrorist financing regime, including problems with correspondent banking, identification of beneficial owners, and the cross-border transportation of currency. The Government of Switzerland should continue to improve on its regime by enacting the revisions developed in response to the FATF mutual evaluation. Switzerland should also continue to work toward full implementation of existing laws and regulations and should ratify the UN Convention against Corruption.

Syria

Syria is not an important regional or offshore financial center, due primarily to its still under-developed private banking sector and the fact that the Syrian pound is not a fully convertible currency. However, there continue to be significant money laundering and terrorism financing vulnerabilities in Syria's financial and nonbank financial sectors that have not been addressed by necessary legislation or other government action. In addition, Syria's black market moneychangers are not adequately regulated, and the country's borders remain porous. Regional hawala networks are intertwined with smuggling and trade-based money laundering and raise significant concerns, including involvement in the finance of terrorism. Most of the indigenous money laundering threat involves Syria's political and business elite, whose corruption and extra-legal activities represent the biggest obstacle to Syria fully choking off money laundering and terrorist financing activities. Syria is ranked 97 out of 163 countries on Transparency International's 2006 Corruption Perception Index. The U.S. Department of State has designated Syria as a State Sponsor of Terrorism.

Syria's free trade zones also may provide an easy entry or transit point for the proceeds of criminal activities. There are seven free zones in Syria, serviced mostly by subsidiaries of Lebanese banks, including BLOM Bank, BEMO (Banque Europeenne Pour le Moyen-Orient Sal), and BBAC (Bank of Beirut and Arab Countries), with four additional public free zones scheduled to begin operation in 2007, including in Homs, Dayr al Zu, the Port of Tartous, and al-Hasakeh near the northeastern segment of the Syrian-Iraqi border.

An Iranian free trade zone is to be co-located within the Homs free trade zone, and a Chinese free trade zone will shortly be operating within the Adra free trade zone. In May 2005 the first private free zone was licensed to be established in al-Kesweh, a Damascus areas suburb, but has not started operations. The volume of goods entering the free zones is estimated to be in the billions of dollars and is growing, especially with the increasing demand for automobiles and automotive parts, which enter the zones free of customs tariffs before being imported into Syria. While all industries and financial institutions in the free zones must be registered with the General Organization for Free Zones, which is part of the Ministry of Economy and Trade, the Syrian General Directorate of Customs continues to lack strong procedures to check country of origin certification or the resources to adequately monitor goods that enter Syria through the zones. There are also continuing reports of Syrians using the free zones to import arms and other goods into Syria in violation of USG sanctions under the Syrian Accountability and Lebanese Sovereignty Act.

The banking sector is dominated by the Commercial Bank of Syria (CBS), which holds approximately 75 percent of all deposits and controls most of the country's foreign currency reserves. With growing competition from the private banks, the CBS and the country's four other specialized public banks—the Agricultural Cooperative Bank, the Industrial Bank, the Real Estate Bank, and the People's Credit Bank—have been preparing a broader range of retail services and more competitive interest rates.

However, these banks still primarily focus on financing Syria's ill-performing public enterprises. In April 2006 the U.S. Department of Treasury issued a final ruling that imposes a special measure against the CBS, along with its subsidiary, the Syrian Lebanese Commercial Bank, as a financial institution of "primary money laundering concern," pursuant to Section 311 of the USA PATRIOT Act, due to information that the CBS has been used by terrorists or persons associated with terrorist organizations, as a conduit for the laundering of proceeds generated from the illicit sale of Iraqi oil, and continued concerns that the CBS is exploited by criminal enterprises.

The Syrian Arab Republic Government (SARG) began taking steps to develop a private banking sector in April 2001, with Law No. 28, which legalized private banking, and Law No. 29, which established rules on bank secrecy. Bank of Syria and Overseas, a subsidiary of Lebanon's BLOM Bank, was the first private bank to open in Syria in January 2004. There are now seven private banks, including Banque BEMO Saudi Fransi, the International Bank for Trade and Finance, Bank Audi,

Arab Bank, Byblos Bank, and Syria Gulf Bank. The sector's total capitalization is more than approximately $300 million, reported an approximate 95 percent in growth in 2006 in their deposit accounts, and are playing an increasing role in providing the business sector with foreign currency to finance imports and as a source of credit for businesses and individuals. However, the sector's development is hampered by the continuing lack of human capacity in the finance sector, regulations that limit Syrian banks' ability to make money on their liquidity, and restrictions on foreign currency transactions. A new law was enacted in May 2005 that allows for the establishment of Islamic banks, and three have already obtained licenses, including the Syrian International Islamic Bank, the Al-Sham Islamic Bank, and the Al-Baraka Bank. While these Islamic banks are expected to begin operations by early 2007, they potentially face problems because of the lack of an adequate regulatory and auditing structure in Syria's finance sector.

Legislation approved in the last few years provides the Central Bank of Syria with new authority to oversee the banking sector and investigate financial crimes. The SARG passed Decree 59 in September 2003 to criminalize money laundering and create an Anti-Money Laundering Commission (Commission), which was established in May 2004. In response to international pressure to improve its anti-money laundering and counterterrorism financing (AML/CTF) regulations, the SARG passed Decree 33 in May 2005, which strengthens the Commission and empowers it to act as a Financial Intelligence Unit (FIU). The Decree finalized the Commission's composition to include the Governor of the Central Bank, a Supreme Court Judge, the Deputy Minister of Finance, the Deputy Governor for Banking Affairs, the SARG's Legal Advisor, and will include the Chairman of the Syrian Stock Market once the Market is operational.

Under Decree 33, all banks and nonfinancial institutions are required to file Suspicious Activity Reports (SARs) with the Commission for transactions over $10,000, as well as suspicious transactions regardless of amount. They are also required to use "know your customer" (KYC) procedures to follow up on their customers every three years and maintain records on closed accounts for five years. The chairmen of Syria's private banks continue to report that they are employing internationally recognized KYC procedures to screen transactions and also employ their own investigators to check suspicious accounts. Nonbank financial institutions must also file SARs with the Commission, but many of them continue to be unfamiliar with the requirements of the law. The Commission has organized workshops for these institutions over the past year, but more time is needed for the information to penetrate the market.

Once a SAR has been filed, the Commission has the authority to conduct an investigation, waive bank secrecy on specific accounts to gather additional information, share information with the police and judicial authorities, and direct the police to carry out a criminal investigation. In addition, Decree 33 empowers the Governor of the Central Bank, who is the chairman of the Commission, to share information and sign Memoranda of Understanding (MOUs) with foreign FIUs. In November 2005, the Prime Minister announced that the Commission had completed an internal reorganization, creating four specialized units to: oversee financial investigations; share information with other SARG entities including customs, police and the judiciary; produce AML/CTF guidelines and verify their implementation; and develop a financial crimes database.

Decree 33 provides the Commission with a relatively broad definition of what constitutes a crime of money laundering, but one that does not fully meet international standards. The definition includes acts that attempt to conceal the proceeds of criminal activities, the act of knowingly helping a criminal launder funds, and the possession of money or property that resulted from the laundering of criminal proceeds. In addition, the law specifically lists thirteen crimes that are covered under the AML legislation, including narcotics offenses, fraud, and the theft of material for weapons of mass destruction. It is unclear whether terrorist financing is a predicate offense for money laundering or otherwise punishable under Decree 33.

While a SAR is being investigated, the Commission can freeze accounts of suspected money launderers for a nonrenewable period of up to eighteen days. The law also stipulates the sanctions for convicted money launderers, including a three to six-year jail sentence and a fine that is equal to or double the amount of money laundered. Further, the law allows the SARG to confiscate the money and assets of the convicted money launderer. The Commission circulates among its private and public banks the names of suspected terrorists and terrorist organizations listed on the UNSCR 1267 Sanction Committee's consolidated list, and it has taken action to freeze the assets of designated individuals, including freezing the assets of one Syrian individual listed on the 1267 list in 2006.

In the first 11 months of 2006, the Commission reported 162 suspicious transactions cases, 24 from banks, up from approximately 90 cases in 2005. The Commission has investigated and sent approximately 5 cases from 2005 and 33 cases in 2006 to the court system; however, all of these cases are still pending and there have not yet been arrests or convictions. Most Syrian judges are not yet familiar with the evidentiary requirements of the law. Furthermore, the slow pace of the Syrian legal system and political sensitivities are delaying quick adjudication of these issues. The Commission itself continues to be seriously hampered by human resource constraints, although it has increased its staff from six in 2005 to ten in 2006, and hopes to expand to 30 by the end of 2007. The Commission has also organized multiple training sessions, including with the World Bank, over the course of 2006, in Syria and abroad, on issues of AML/CTF detection. A small number of customs officials attended these sessions. However, the lack of expertise on AML/CTF issues, further undermined by a lack of political will, continues to impede effective implementation of existing AML/CTF regulations.

Although Decree 33 provides the Central Bank with a foundation to combat money laundering, most Syrians still do not maintain bank accounts or use checks, credit cards, or ATM machines. The Syrian economy remains primarily cash-based, and Syrians use moneychangers, some of whom also act as hawaladars, for many financial transactions. Estimates of the volume of business conducted in the black market by Syrian moneychangers range between $15-70 million a day. Even the SARG admits that it does not have visibility into the amount of money that currently is in circulation. The SARG has begun issuing new regulations to entice people to use the banking sector, including offering high interest certificates of deposit and allowing Syrians to access more foreign currency from banks when they are traveling abroad. The SARG also passed a Moneychangers Law in 2006 to try to regulate the sector, requiring moneychangers to receive a license. However, it is unlikely that black market currency transactions will enter the formal sector because the SARG has still not offered adequate incentives; there is a 25 percent tax on these transactions, inadequate enforcement mechanisms, and continuing restrictions on foreign currency transfers. The Commission does have the authority to monitor the sector under Decree 33, but it reports that as moneychangers have until the end of 2006 to license their operations, they have not yet begun investigating these operations. The hawaladars in Syria's black market remain a source of concern for money laundering and terrorist financing.

The SARG has not updated its laws regarding charitable organizations to include strong AML/CTF language. A promised updated draft law is still pending. The SARG decided at the end of 2004 to restrict charitable organizations to only distributing nonfinancial assistance, but the current laws do not require organizations to submit detailed financial information or information on their donors. While the Commission says that it is seeking to increase cooperation with the Ministry of Social Affairs and Labor, which is supposed to approve all charitable transactions, to-date this remains a largely unregulated area.

While the SARG maintains strict controls on the amount of money that individuals can take with them out of the country, there is a high incidence of cash smuggling across the Lebanese, Iraqi, and Jordanian borders. Most of the smuggling involves the Syrian pound, as a market for Syrian currency exists among expatriate workers and tourists in Lebanon, Jordan, and the Gulf countries. U.S. dollars are also commonly smuggled in the region. Some of the smuggling may involve the proceeds of narcotics and other criminal activity. In addition to cash smuggling, there also is a high rate of

commodity smuggling out of Syria, particularly of diesel fuel, prompted by individuals buying diesel domestically at the low subsidized rate and selling it for much higher prices in neighboring countries. There are reports that some smuggling is occurring with the knowledge of or perhaps even under the authority of the Syrian security services.

The General Directorate of Customs lacks the necessary staff and financial resources to effectively handle the problem of smuggling. And while it is has started to enact some limited reforms, including the computerization of border outposts and government agencies, problems of information-sharing remain. Customs also announced in 2005 that it planned to develop a special office to combat AML/CTF in coordination with the Ministry of Finance and Syria's security services, but this has not yet become operational. Additionally, Customs currently lacks the infrastructure to effectively monitor or control even the legitimate movement of currency across its borders. The Commission and Customs have developed a joint form for individuals to declare currency when entering or exiting the country, but it has not yet been implemented. Additionally, once the new form is in place, it will remain a voluntary procedure. To combat corruption among customs officers, the General Directorate of Customs announced in December 2005 that it planned to ban all cash transactions at the borders, including the payment of customs duties, and will replace cash transactions with a system that utilizes pre-paid cards; however these programs have still not been realized.

Syria is one of the fourteen founding members of the Middle East and North Africa Financial Action Task Force (MENAFATF), a FATF-style regional body. In 2006, Syria underwent a mutual evaluation by its peers in MENAFATF which will be released shortly. Syria participated as an observer at the Egmont Group meeting in June 2006 and has formally applied to become a full member. Syria is a party to the 1988 UN Drug Convention. In April 2005, it became a party to the International Convention on the Suppression of the Financing of Terrorism. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime.

While Syria has made some effort in 2006 to implement AML/CTF regulations that govern its formal financial sector, including ratifying a law to regulate black market currency transactions, nonbank financial institutions and the black market continue to be vulnerable to money laundering and terrorist financiers. Syria should continue to modify its AML/CTF legislation and enabling regulations so that they adhere to global standards. The General Directorate of Customs, the Central Bank, and the judicial system in particular continue to lack the resources and the political will to effectively implement AML/CTF measures. Although the SARG has stated its intention to create the technical foundation through which different government agencies could share information about financial crimes, this does not exist to date. Syria should ratify the UN Convention against Transnational Organized Crime. It should criminalize terrorist financing. In addition, it is doubtful that the SARG has the political will to punish terrorist financing, to classify what it sees as legitimate resistance groups as terrorist organizations, or to address the corruption that exists at the highest levels of government and business. All these issues remain obstacles to developing a comprehensive and effective AML/CTF regime in Syria.

Taiwan

Taiwan's modern financial sector and its role as a hub for international trade make it susceptible to money laundering. Its location astride international shipping lanes makes it vulnerable to transnational crimes such as narcotics trafficking and smuggling. There is a significant volume of informal financial activity through unregulated nonbank channels. Most illegal or unregulated financial activities are related to tax evasion, fraud, or intellectual- property violations. According to suspicious activity reports (SARs) filed by financial institutions on Taiwan, the predicate crimes commonly linked to SARs include financial crimes, corruption, and other general crimes.

Taiwan's anti-money laundering legislation is embodied in the Money Laundering Control Act (MLCA) of April 23, 1997, which was amended in 2003. Its major provisions include a list of predicate offenses for money laundering, customer identification and record keeping requirements, disclosure of suspicious transactions, international cooperation, and the creation of a financial intelligence unit, the Money Laundering Prevention Center (MLPC). In 2006, the Ministry of Justice began drafting another amendment to the MLCA, which would revise the scope of predicate crimes for money laundering, among other proposed changes.

The Legislative Yuan (parliament) amended the MLCA in 2003 to expand the list of predicate crimes for money laundering, widen the range of institutions subject to suspicious transaction reporting, and mandate compulsory reporting to the MLPC of significant currency transactions of over New Taiwan Dollars (TDW)1 million (approximately $30,000). Between August 2003, when the amended MLCA came into force, and May 31, 2004, the MLPC received over one million such reports on currency transactions-with 99 percent of them reported electronically. In 2005, the MLPC received 1,028,834 currency transaction reports. As a result of the 2003 MLCA amendments, the list of institutions subject to reporting requirements was expanded, to include casinos, automobile dealers, jewelers, boat and plane dealers, real estate brokers, credit cooperatives, consulting companies, insurance companies, and securities dealers, as well as traditional financial institutions.

Taiwan also set up a single financial regulator, the Financial Supervisory Commission (FSC) on July 1, 2004. The FSC consolidates the functions of regulatory monitoring for the banking, securities, futures and insurance industries, and also conducts financial examinations across these sectors. In mid-December 2005, the FSC began an incentive program for the public to provide information on financial crimes. The reward for information on a financial case with fines of TDW 10 million (approximately $300,000) or at least a one-year sentence is up to TDW 500,000 (approximately $15,000). The reward for information on a case with a fine of between TDW 2-10 million (approximately $60,000-$300,000) or less than a one-year sentence is up to TDW 200,000 (approximately $6,000).

Two new articles added to the 2003 amendments to the MLCA granted prosecutors and judges the power to freeze assets related to suspicious transactions and gave law enforcement more powers related to asset forfeiture and the sharing of confiscated assets. The proposed second amendment to the MLCA would prolong the permitted period of freezing the proceeds of money laundering from 6 months to 1 ½ years. In terms of reporting requirements, financial institutions are required to identify, record, and report the identities of customers engaging in significant or suspicious transactions. There is no threshold amount specified for filing suspicious transaction reports. The time limit for reporting cash transactions of over TDW 1 million (approximately $39,000) is within five business days. Banks are barred from informing customers that a suspicious transaction report has been filed. Reports of suspicious transactions must be submitted to the MLPC within 10 business days after the transaction took place. From January to October 2006, the MLPC received 1,085 suspicious transaction reports and 443 of them resulted in prosecutions.

Institutions are also required to maintain records necessary to reconstruct significant transactions, for an adequate amount of time. Bank secrecy laws are overridden by anti-money laundering legislation, allowing the MPLC to access all relevant financial account information. Financial institutions are held responsible if they do not report suspicious transactions. In May 2004, the Ministry of Finance issued instructions requiring banks to demand two types of identification and to retain photocopies of the identification cards when bank accounts are opened upon request for a third party, in order to prove the true identity of the account holder. Individual bankers can be fined TDW 200,000-1 million ($7,800-$39,000) for not following the MLPA.

All foreign financial institutions and offshore banking units follow the same regulations as domestic financial entities. Offshore banks, international businesses, and shell companies must comply with the

disclosure regulations from the Central Bank, Bureau of Monetary Affairs (CB), and MLPC. These supervisory agencies conduct background checks on applicants for banking and business licenses. Offshore casinos and internet gambling sites are illegal. According to Taiwan's Central Bank of China (CBC), from January to August 2006, Taiwan hosted 33 local branches of foreign banks, two trust and investment companies, and 67 offshore banking units.

On January 5, 2006, the Offshore Business Unit (OBU) Amendment was ratified to allow expansion of OBU operations to the same scope as Domestic Business Units (DBU). This was done to assist China-based Taiwan businesspeople in financing their offshore business operations. DBUs engaging in cross-strait financial business must follow the regulations of the "Act Governing Relations between Peoples of the Taiwan Area and the Mainland Area" and "Regulations Governing Approval of Banks to Engage in Financial Activities between the Taiwan Area and the Mainland Area." The Competent Authority, as referred to in these Regulations, is the Ministry of Finance.

Taiwan prosecuted 688 cases involving money laundering from January to October 2006, compared with 947 cases involving financial crimes during the same period of 2005. Among the 688 cases, 631 involved unregistered stock trading, credit card theft, currency counterfeiting or fraud. Among the 57 other money laundering cases, 11 were corruption-related and one was drug-related.

Individuals are required to report currency transported into or out of Taiwan in excess of TDW 60,000 (approximately $1,850); or $10,000 in foreign currency; 20,000 Chinese renminbi; or gold worth more than $20,000. When foreign currency in excess of TDW 500,000 (approximately $15,400) is brought into or out of Taiwan, the bank customer is required to report the transfer to the Central Bank, though there is no requirement for Central Bank approval prior to the transaction. Prior approval is required, however, for exchanges between New Taiwan dollars and foreign exchange when the amount exceeds $5 million for an individual resident and $50 million for a corporate entity. Effective September 2003, the Directorate General of Customs assumed responsibility for providing the MLPC on a monthly basis with electronic records of travelers entering and exiting the country carrying any single foreign currency amounting to TDW 1.5 million (approximately $58,500). Starting August 1, 2006, those who transfer funds over TDW 30,000 at any bank in Taiwan must produce a photo ID and the bank must record the name, ID number and telephone number of the client.

The authorities on Taiwan are actively involved in countering the financing of terrorism. In 2003, a new "Counter-Terrorism Action Law" (CTAL) was drafted, although as of July 2006 it was still under review by the Legislative Yuan. The new law would explicitly designate the financing of terrorism as a major crime. Under the proposed CTAL, the National Police Administration, the MJIB, and the Coast Guard would be able to seize terrorist assets even without a criminal case in Taiwan. Also, in emergency situations, law enforcement agencies would be able to freeze assets for three days without a court order.

Assets and income obtained from terrorist-related crimes could also be permanently confiscated under the proposed CTAL, unless the assets could be identified as belonging to victims of the crimes. Taiwan officials currently have the authority to freeze and/or seize terrorist-related financial assets under the MLCA promulgated in 1996 and amended in February 2003 to cover terrorist finance activities. Under the Act, the prosecutor in a criminal case can initiate freezing assets, or without criminal charges, the freezing/seizure can be done in response to a request made under a treaty or international agreement.

The Bureau of Monetary Affairs (BOMA) has circulated to all domestic and foreign financial institutions in Taiwan the names of individuals and entities included on the UN 1267 Sanctions Committee's consolidated list. Taiwan and the United States have established procedures to exchange records concerning suspicious terrorist financial activities. After receiving financial terrorist lists from the American Institute in Taiwan, BOMA conveys the list to relevant financial institutions. Banks are required to file a report on cash remittances if the remitter/remittee is on a terrorist list. Although as

noted above Taiwan does not yet have the authority to confiscate the assets, the MLCA was amended to allow the freezing of accounts suspected of being linked to terrorism.

Alternative remittance systems, or underground banks, are considered to be operating in violation of Banking Law Article 29. Authorities in Taiwan consider these entities to be unregulated financial institutions. Foreign labor employment brokers are authorized to use banks to remit income earned by foreign workers to their home countries. These remittances are not regulated or reported. Thus, money laundering regulations are not imposed on these foreign labor employment brokers. However, if the brokers accept money in Taiwan dollars for delivery overseas in another currency, they are violating Taiwan law. It is also illegal for small shops to accept money in Taiwan dollars and remit it overseas. Violators are subject to a maximum of three years in prison, and/or forfeiture of the remittance and/or a fine equal to the remittance amount.

Authorities in Taiwan do not believe that charitable and nonprofit organizations in Taiwan are being used as conduits for the financing of terrorism, and there are currently no plans to investigate such entities further for terrorist financing. Such organizations are required to register with the government. The Ministry of Interior (MOI) is in charge of overseeing foundations and charities. In 2004 and in 2006, the MOI assigned public accountants to audit the financial management of nationwide foundations.

Article 3 of Taiwan's Free Trade Zone Establishment and Management Act defines a Free Trade Zone (FTZ) as a controlled district of an international airport or an international seaport approved by the Executive Yuan. The FTZ coordination committee, formed by the Executive Yuan, has the responsibility of reviewing and examining the development policy of the FTZ; the demarcation and designation of FTZs; and inter-FTZ coordination.

There are five FTZs in Taiwan which have opened since 2004, including Taipei Free Trade Zone, Taichung Free Trade Zone, Keelung Free Trade Zone, Kaohsiung Free Trade Zone, and Taoyuan Air Cargo Free Trade Zone. These FTZs were designated with different functions, so that Keelung and Taipei FTZs focus on international logistics; Taoyuan FTZ on adding value to high value added industries; Taichung FTZ on warehousing, transshipment and processing of cargo; and Kaohsiung FTZ on mature industrial clusters. According to the Center for Economic Deregulation and Innovation (CEDI) under the Council for Economic Planning & Development, by September 2006 there were 11 shipping and logistics companies listed in the Kaohsiung Free Trade Zone, seven logistics companies in Taichung Free Trade Zone, eight logistics and shipping companies in Keelung Free Trade Zone, one logistics company in Taipei Free Trade Zone, and 46 manufacturers and enterprises in Taoyuan Air Cargo Free Trade Zone. There is no indication that FTZs in Taiwan are being used in trade-based money laundering schemes or by the financiers of terrorism. According to Article 14 of the Free Trade Establishment and Management Act, any enterprise applying to operate within an FTZ shall apply to the management authorities of the particular FTZ by submitting a business operation plan, the written operational procedures for good control, customs clearance, and accounting operations, together with relevant required documents. Financial institutions may apply to establish a branch office inside the FTZ and conduct foreign exchange business, in accordance with the Banking Law of the ROC, Securities and Exchange Law, Statute Governing Foreign Exchange, and the Central Bank of China Act.

According to Taiwan's Banking Law and Securities Trading Law, in order for a financial institution to conduct foreign currency operations, Taiwan's Central Bank must first grant approval. The financial institution must then submit an application to port authorities to establish an offshore banking unit (OBU) in the free-trade zone. No financial entity has yet applied to establish such an OBU in any of the five free trade zones. An offshore banking unit may operate a related business under the Offshore Banking Act, but cannot conduct any domestic financial, economic, or commercial transaction in New Taiwan Dollars.

Taiwan has promulgated drug-related asset seizure and forfeiture regulations which provide that in accordance with treaties or international agreements, Taiwan's Ministry of Justice shall share seized assets with foreign official agencies, private institutions or international parties that provide Taiwan with assistance in investigations or enforcement. Assets of drug traffickers, including instruments of crime and intangible property, can be seized along with legitimate businesses used to launder money. The injured parties can be compensated with seized assets. The Ministry of Justice distributes other seized assets to the prosecutor's office, police or other anti-money laundering agencies. The law does not allow for civil forfeiture. In March, 2006, Taiwan authorities announced that they had confiscated $625 million, arrested 22 men and had frozen approximately NT$1.7 billion ($438 million), in the island's largest money laundering operation, A mutual legal assistance agreement between the American Institute in Taiwan (AIT) and the Taipei Economic and Cultural Representative Office in the United States (TECRO) entered into force in March 2002. It provides a basis for the law enforcement agencies of the people represented by AIT and TECRO to cooperate in investigations and prosecutions for narcotics trafficking, money laundering (including the financing of terrorism), and other financial crimes.

Although Taiwan is not a UN member and cannot be a party to the 1988 UN Drug Convention, the authorities in Taiwan have passed and implemented laws in compliance with the goals and objectives of the Convention. Similarly, Taiwan cannot be a party to the UN International Convention for the Suppression of the Financing of Terrorism, as a nonmember of the United Nations, but it has agreed unilaterally to abide by its provisions. Taiwan is a founding member of the Asia/Pacific Group on Money Laundering (APG) and in 2005, was elected to the APG steering committee. The MLPC is a member of the Egmont Group of Financial Intelligence Units. The Investigation Bureau of the Ministry of Justice expanded information exchanges with various countries/jurisdictions from 17 jurisdictions in 2004 to 20 in 2005.

Over the past five years, Taiwan has created and implemented an anti-money laundering regime that comports with international standards. The MLCA amendments of 2003 address a number of vulnerabilities, especially in the area of asset forfeiture. The authorities on Taiwan should continue to strengthen the existing anti-money laundering regime as they implement the new measures. Taiwan should endeavor to pass the proposed Counter-Terrorism Action Law to better address terrorist financing issues. The authorities on Taiwan should also enact legislation regarding alternate remittance systems. Taiwan should enact legislation pending since 2003 that explicitly criminalizes the financing of terrorism.

Tanzania

Tanzania is not an important regional financial center. Tanzania, however, is vulnerable to money laundering. Tanzania has weaknesses in its anti-money laundering/counterterrorism financing (AML/CTF) regime, specifically in its financial institutions and law enforcement capabilities. A weak financial sector along with an under-trained, under-funded law enforcement apparatus and the lack of a functioning financial intelligence unit (FIU) make money laundering impossible to track and prosecute. Real estate and used car businesses appear to be vulnerable trade industries involved in money laundering. With little or lax regulations and enforcement, the emerging casino industry is becoming an area of concern for money laundering. Money laundering is even more likely to occur in the informal nonbank financial sector, as opposed to the formal sector, which is largely undeveloped. Front companies are used to launder funds including hawaladars and bureaux de change, especially on the island of Zanzibar, where few federal regulations apply. Officials indicate that money laundering schemes in Zanzibar generally take the form of foreign investment in the tourist industry and bulk cash smuggling. The likely sources of illicit funds are from Asia and the Middle East and, to a lesser extent, Europe. Such transactions rarely include significant amounts of U.S. currency. There are no

indications that Tanzania's two free trade zones are being used in trade-based money laundering schemes or by financiers of terrorism.

The Proceeds of Crime Act of 1991 criminalizes narcotics-related money laundering; however, the Act does not adequately define money laundering. The law has been used only to prosecute corruption cases and over the past year there have been no arrests or prosecutions for money laundering or terrorist financing. The law requires financial institutions to maintain records of financial transactions exceeding 100,000 shillings (approximately $109) for a period of 10 years.

Current law does not include due diligence or negligence laws for banks. If an institution has reasonable grounds to believe that a transaction relates to money laundering, it may communicate this information to the police for investigation, although such reporting is voluntary, not mandatory. The Central Bank, the Bank of Tanzania (BOT), has issued regulations requiring financial institutions to file suspicious transaction reports (STRs), but this requirement is not being enforced, and no mechanism currently exists for receiving and analyzing the STRs.

The 2002 Prevention of Terrorism Act criminalizes terrorist financing. It requires all financial institutions to inform the government each quarter in a calendar year of any assets or transactions that may be associated with a terrorist group. The implementing regulations for this provision have not yet been drafted. Under the Act, the government may seize assets associated with terrorist groups. The BOT circulates to Tanzanian financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanction Committee's consolidated list, but to date no assets have been frozen under this provision. In 2004, the Government of Tanzania (GOT) took action against one charitable organization on the list by closing its offices and deporting its foreign directors; however, it is not clear whether Tanzania has the investigative capacity to identify and seize related assets. Tanzania has cooperated with the U.S. in investigating and combating terrorism and exchanges counterterrorism information. There are no specific laws in place allowing Tanzania to exchange records with the U.S. on narcotics transactions or narcotics-related money laundering.

Tanzania made progress in 2006 with its proposed anti-money laundering (AML) legislation. The national multi-disciplinary committee, established with the help of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), finalized the AML bill in 2005 after gaining input from a wide range of stakeholders. In June 2006, President Kikwete's Cabinet approved the AML bill and tabled it in Parliament. Reportedly, officials expect Parliament to pass the bill by February 2007. Among its other provisions, the proposed legislation provides for the creation of a FIU that will collect mandatory suspicious transaction reporting from financial institutions and will be empowered to share this information with other FIUs and foreign law enforcement agencies.

Money laundering controls and reporting requirements do not currently apply to nonbank financial institutions, such as cash couriers, casinos, hawaladars and bureaux de change. The draft AML bill includes the expansion of money laundering controls to cover such institutions. Currently, the BOT supervises bureaux de change through the use of annual audits and inspections, while the National Gaming Authority supervises casinos and other gaming activities involving large sums of money, including lotteries. There are no legal requirements for nonbank financial institutions to report suspicious transactions. There is currently no cross-border currency reporting requirement, even for cash couriers, although the Proceeds of Crime Act does characterize cash smuggling as a "predicate offense." The draft AML bill includes strengthened provisions to criminalize cash smuggling in and out of Tanzania.

The GOT is a party to the 1988 UN Drug Convention; the UN International Convention for the Suppression of the Financing of Terrorism; and the UN Convention Against Corruption. In May 2006, the GOT became a party to the UN Convention against Transnational Organized Crime. In 2006, Tanzania was listed 93 out of 163 countries in Transparency International's Corruption Perception Index. Tanzania is a member of ESAAMLG and continues to play a leading role in the operation of

this FATF-style regional body. Tanzania also continues to host the annual ESAAMLG task force meetings and has detailed personnel to the ESAAMLG Secretariat which it hosts.

The Government of Tanzania should enact and implement the anti-money laundering law that has been under review for several years. Tanzania should also increase the reporting requirements for informing the government of assets or transactions that may be associated with a terrorist group. Currently the GOT requires quarterly reporting requirements regarding terrorist financing. The importance of stopping terrorist acts should mandate a shorter reporting interval in this arena. The GOT should continue to work through the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) to establish the FIU mandated in the draft law and to develop a comprehensive anti-money laundering regime that comports with international standards. Per the Financial Action Task Force Special Recommendation Nine, the GOT should enact mandatory cross-border currency reporting requirements. Tanzania should also enact and enforce anti-money laundering regulations within the casino industry.

Thailand

Thailand is vulnerable to money laundering from its significant underground economy as well as from all types of cross-border crime including illicit narcotics, contraband, and smuggling. Money launderers use both the banking and nonbanking financial institutions and private businesses to move funds from narcotics trafficking and other criminal enterprises. As the amount of opium and heroin produced in the Golden Triangle region of Burma, Laos, and Thailand decreased during the past decade, drug traffickers transitioned to importing and distributing methamphetamine tablets, and began using commercial banks to hide and move their proceeds. Thailand is a significant destination and source country for international migrant smuggling and trafficking in persons, a production and distribution center for counterfeit consumer goods, and increasingly a center for the production and sale of fraudulent travel documents. Banks and alternative remittance systems are illegally used to shelter and move funds produced by all of these activities as well as by illegal gambling and prostitution. The majority of reported money laundering cases is narcotics-related, and there is no pervasive evidence of money laundering ties in Thailand with international terrorist groups. The Thai black market for smuggled goods includes pirated goods as well as automobiles from neighboring nations.

Thailand's anti-money laundering legislation, the Anti-Money Laundering Act (AMLA) B.E. 2542 (1999), criminalizes money laundering for the following predicate offenses: narcotics trafficking, trafficking in women or children for sexual purposes, fraud, financial institution fraud, public corruption, customs evasion, extortion, public fraud, blackmail, and terrorist activity. On August 11, 2003, as permitted by the Thai constitution, the Royal Thai Government (RTG) issued two Emergency Decrees to enact measures related to terrorist financing that had been under consideration by the Executive Branch and Parliament for more than a year and a half. The first of these Decrees amended Section 135 of the Penal Code to establish terrorism as a criminal offense. The second Decree amended Section 3 of the AMLA to add the newly established offense of terrorism and terrorist financing as an eighth predicate offense for money laundering. The Decrees took effect when they were published. Parliament endorsed their status as legal acts in April 2004.

The current list of predicate offenses in the AMLA does not comport with international best practices, consistent with Recommendations 1 and 2 of the Forty Recommendations of the Financial Action Task Force (FATF), to apply the crime of money laundering to all serious offenses or with the minimum list of acceptable designated categories of offenses. Additionally, the definition of "property involved in an offense" in the AMLA is limited to proceeds of predicate offenses and does not extend to instrumentalities of a predicate offense or a money laundering offense. Proposed amendments pending with the Cabinet since 2004 would expand the list of predicate offenses to include

environmental crimes, foreign exchange violations, illegal gambling, arms trafficking, labor fraud, bid rigging, share manipulation, and excise tax offenses. However, even with the enactment of these additional predicate offenses, the list will still be deficient under international standards as it excludes, among other crimes, murder, migrant smuggling, counterfeiting, and intellectual property rights offenses. The proposed amendments to AMLA would also create a forfeiture fund and authorize international asset sharing with cooperating jurisdictions.

The AMLA created the Anti-Money Laundering Office (AMLO). Among other functions it serves as Thailand's financial intelligence unit (FIU), which became fully operational in 2001. When first established, AMLO reported directly to the Prime Minister. In October 2002, pursuant to a reorganization of the executive branch following criticisms that AMLO had been politicized, AMLO was designated as an independent agency under the Minister of Justice. AMLO receives, analyzes, and processes suspicious and large transaction reports, as required by the AMLA. In addition, AMLO is responsible for investigating money laundering cases for civil forfeiture and for the custody, management, and disposal of seized and forfeited property. AMLO is also tasked with providing training to the public and private sectors concerning the AMLA. The law also created the Transaction Committee, which operates within AMLO to review and approve disclosure requests to financial institutions and asset restraint/seizure requests. The AMLA also established the Anti-Money Laundering Board, which is comprised of ministerial-level officials and agency heads and serves as an advisory board that meets periodically to set national policy on money laundering issues and to propose relevant ministerial regulations.

AMLO, the Royal Thai Police (RTP) Special Branch, and the Royal Thai Police Crimes Suppression Division are responsible for investigating financial crimes. They initiated 1,215 financial crimes investigations in 2005 resulting in a total of 57 convictions. During the 2006 fiscal year (10/05-09/06), AMLO prosecuted 79 cases of civil asset forfeiture and realized Bt459 million or $11.8 million. Eleven cases remain under investigation. In criminal cases, the forfeiture and seizure of assets is governed by the 1991 Act on Measures for the Suppression of Offenders in an Offense relating to Narcotics (Assets Forfeiture Law). The Property Examination Committee has filed 1,865 cases with assets valued at 1.64 billion baht (approximately $4 million) and 1,644 cases are on trial. Thai authorities seized the equivalent of $18.7 million in nonterrorist assets during 2005, compared to $16.52 million in 2004, and $56.3 million in 2003. The high success rate in 2003 occurred during the Prime Minister's much-criticized war on drugs that year, in which more than 2,000 extra-judicial killings occurred.

The Ministry of Justice also houses a criminal investigative agency, the Department of Special Investigations (DSI), which is separate from the RTP although many DSI personnel originally were RTP officers. DSI has responsibility for investigating the criminal offense of money laundering (as distinct from civil asset forfeiture actions carried out by AMLO), and for many of the money laundering predicates defined by the AMLA, including terrorism. The DSI, AMLO, and the RTP all have authority to identify, freeze, and/or forfeit terrorist finance-related assets.

AMLO shares information with other Thai law enforcement agencies and vice versa. It has a memorandum of understanding with the Royal Thai Customs, pursuant to which Royal Thai Customs shares information and evidence of smuggling and customs evasion involving goods or cash exceeding Bt 1 million (approximately USD25,600).

The AMLA requires customer identification, record keeping, the reporting of large and suspicious transactions, and provides for the civil forfeiture of property involved in a money laundering offense. Financial institutions are also required to keep customer identification and specific transaction records for a period of five years from the date the account was closed, or from the date the transaction occurred, whichever is longer. Reporting individuals (banks and others) who cooperate with law enforcement entities are protected from liability. Thailand does not have stand-alone secrecy laws but

the Commercial Bank Act B.E. 2505 (1962), regulated by Bank of Thailand, has a provision providing for bank secrecy to prevent disclosure of client financial information. However, AMLA overrides this provision. Therefore, financial institutions must disclose their client and ownership information to AMLO if requested. .

The Bank of Thailand (BOT), Securities and Exchange Commission (SEC), and AMLO are empowered to supervise and examine financial institutions for compliance with anti-money laundering/counterterrorist financial laws and regulations. Although the Bank of Thailand regulates financial institutions in Thailand, bank examiners are prohibited, except under limited circumstances, from examining the financial transactions of a private individual. This prohibition acts as an impediment to the BOT's auditing of a financial institution's compliance with the AMLA or BOT regulations. Besides this lack of power to conduct transactional testing, BOT does not currently examine its financial institutions for anti-money laundering compliance. The BOT is working closely with AMLO to train officers in conducting compliance audits, and in 2007 AMLO is expecting to setup an on-and-off site audit team with assistance from the BOT, although no such audits have yet to occur.

Anti-money laundering controls are also enforced by other Royal Thai Government regulatory agencies, including the Board of Trade and the Department of Insurance. Financial institutions that are required to report suspicious activities are broadly defined by the AMLA as any business or juristic person undertaking banking or nonbanking business. The land registration offices are also required to report on any transaction involving property of Bt5 million or greater, or a cash payment of Bt2 million or greater, for the purchase of real property.

The Exchange Control Act of B.E. 2485 (1942) states that foreign currencies can be brought into Thailand without limit. However, any person receiving foreign currencies is required to surrender foreign currencies to an authorized bank or to deposit the same in a foreign currency account within 7 days from receipt, except foreigners temporarily staying in Thailand for not more than three months, foreign embassies, and international organizations. (In November 2006, the BOT amended the surrender period from 7 days to 15 days but the amendment is pending the Ministry of Finance's approval.) Meanwhile, there is no restriction on the amount of Thai currency (Baht) that may be brought into the country. However, a person traveling to Thailand's bordering countries including Vietnam is allowed to take out Thai Baht up to Bt500,000 or $12,820 and to other countries up to Bt50,000 ($1,282) without authorization.

Thailand is not an offshore financial center nor does it host offshore banks, shell companies, or trusts. Licenses were first granted to Thai and foreign financial institutions to establish Bangkok International Banking Facilities (BIBFs) in March 1993. BIBFs may perform a number of financial and investment banking services, but can only raise funds offshore (through deposits and borrowing) for lending in Thailand or offshore. The United Nations Drug Control Program and the World Bank listed BIBFs as potentially vulnerable to money laundering activities, because they serve as transit points for funds. BIBFs are subject to the AMLA. However, in mid October 2006, the last BIBF license was returned to the Bank of Thailand due to the BOT's "one presence" policy for all financial institutions. Some of these qualified stand alone BIBFs have upgraded to either full branches or subsidiaries, while Thai commercial banks with BIBF licenses had to surrender their licenses to the BOT. Most BIBFs simply exited the market.

The Stock Exchange of Thailand (SET) requires securities dealers to have "know your customer" procedures; however, the SET does not check anti-money laundering compliance during its reviews. The Department of Insurance (DOI), under the Ministry of Commerce, is responsible for the supervision of insurance companies, which are covered under the AMLA definition of a financial institution, but there are no anti-money laundering regulations for the insurance industry. Similarly, the Cooperative Promotion Department (CPD) is responsible for supervision of credit cooperatives,

which are required under the Cooperatives Act to register with the CPD. Currently, around 6,000 cooperatives are registered, with approximately 1,348 thrift and credit cooperatives engaged in financial business. Thrift and credit cooperatives are engaged in deposit taking and providing loans to the members, and are covered under the definition of a financial institution, but, as with the securities and insurance sectors, there are no anti-money laundering compliance mechanisms currently in place.

Financial institutions (such as banks, finance companies, savings cooperatives, etc.), land registration offices, and persons who act as solicitors for investors, are required to report significant cash, property, and suspicious transactions. Reporting requirements for most financial transactions (including purchases of securities and insurance) exceeding Bt2 million (approximately $52,000), and property transactions exceeding Bt5 million (approximately $130,000), have been in place since October 2000. In 2007, the AMLO Board will again consider the issuance of an announcement or regulation to subject gold shops, jewelry stores, and car dealers to either mandatory transactional reporting requirements and/or suspicious transactions reporting requirements. Previous proposals would have imposed mandatory reporting requirements regarding transactions with nonregular customers involved in business transactions worth more than Bt1 million (or $25,600) or would have imposed mandatory reporting requirements on shops engaging in annual transactions in excess of Bt 100 million (or $2,560,000). The relevant ministries and regulatory authorities would then issue orders consistent with the AMLO Board pronouncement. Thailand has more than 6,000 gold shops and 1,000 gem traders that would be subject to these reporting requirements.

Thailand acknowledges the existence and use of alternative remittance systems (hawala, etc.) that attempt to circumvent financial institutions. There is a general provision in the AMLA that makes it a crime to transfer, or to receive a transfer, that represents the proceeds of a specified criminal offense (including terrorism). Remittance and money transfer agents, including informal remittance businesses, require a license from the Ministry of Finance. Guidelines issued in August 2004 by the Ministry of Finance and the BOT prescribe that before the grant of a license, both money changers and money transfer agents are subject to onsite examination by the BOT, which also consults with AMLO on the applicant's criminal history and AML record. At present, moneychangers have to report financial transactions to the Anti-Money Laundering Office while remittance agents do not. Licensed agents are subject to monthly transaction reporting and a 3-year record maintenance requirement. At present, there are about 270 authorized moneychangers and five remittance agents. The Bank of Thailand limited in 2004 the annual transaction volume for agents to $60,000 for offices in the Bangkok area and $30,000 for offices located in other areas. Moneychangers frequently act as illegal remittance agents.

Money and property may be seized under Section 3 of the AMLA if derived from commission of a predicate offense, from aiding or abetting commission of a predicate offense, or if derived from the sale, distribution, or transfer of such money or asset. AMLO is responsible for tracing, freezing, and seizing assets. Instruments that are used to facilitate crime such as vehicles or farms (when not proceeds) cannot be forfeited under AMLA and are subject to seizure under the Criminal Asset Forfeiture Act of 1991, and unlike the AMLA, require a criminal conviction as a pre-requisite to a final forfeiture. The AMLA makes no provision for substitute seizures if authorities cannot prove a relationship between the asset and the predicate offense. Overall, the banking community in Thailand provides good cooperation to AMLO's efforts to trace funds and seize/freeze bank accounts.

The Bank of Thailand (BOT) does not have any regulations that give it explicit authorization to control charitable donations, but it is working with AMLO to monitor these transactions under the Exchange Control Act of 1942.

In 2004, Regulations on Payment of Incentives and Rewards in Proceedings Against Assets Under the Anti-Money Laundering Act went into effect in Thailand. Under this system, investigators from AMLO and other investigative agencies receive personal commissions on the property they seize that

is ultimately forfeited. The United States as well as several other countries and international organizations, including the UNODC, have criticized this system of personal rewards on the grounds that it threatens the integrity of its AML regime and creates a conflict of interest by giving law enforcement officers a direct financial stake in the outcome of forfeiture cases. The United States and others have called on the RTG to rescind the reward regulation. Despite continuing promises to end the system of personal commissions to law enforcement officers, Thailand has been disappointingly slow to address and correct this discredited practice. As a consequence, the U.S. Government (USG) has ceased providing training and other assistance to AMLO while the rewards practice remains in place. However, in November 2006, the Minister of Justice recommended that the Prime Minister rescind the reward regulation, and the U.S. is encouraged that appropriate action will occur in early 2007 to eliminate this system.

Thailand is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. It has signed (December 2000), but not yet ratified, the UN Convention against Transnational Organized Crime. It has also signed (December 2003), but not yet ratified the UN Convention against Corruption. Implementing legislation must be enacted before Thailand can ratify either Convention. The RTG has issued instructions to all authorities to comply with UNSCR 1267, including the freezing of funds or financial resources belonging to suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list. To date, Thailand has not identified, frozen, and/or seized any assets linked to individuals or entities included on the UNSCR 1267 Sanctions Committee's consolidated list. However, AMLO has identified some suspicious transaction reports derived from financial institutions as possibly terrorist-related and has initiated investigations of possible terrorist activities using nongovernmental or nonprofit organizations as a front.

Thailand has Mutual Legal Assistance Treaties (MLATs) with 10 countries, including the United States and is a party to the regional ASEAN Mutual Legal Assistance Agreement. AMLO has memoranda of understanding on money laundering cooperation with 27 other financial intelligence units (Belgium, Brazil, Lebanon, Indonesia, Romania, UK, Finland, Republic of Korea, Australia, Portugal, Andorra, Estonia, Italy, Philippines, Poland, Mauritius, Netherlands, Georgia, Monaco, Malaysia, Bulgaria, St. Vincent and the Grenadines, Ukraine, Myanmar, Nigeria, Japan, and Ireland). AMLO is currently pursuing FIU agreements with 15 more FIUs. It nonetheless actively exchanges information with nations with which it has not entered into an MOU, including the United States, Singapore, and Canada. Thailand cooperates with USG and other nations' law enforcement authorities on a range of money laundering and illicit narcotics related investigations. AMLO responded to 99 requests for information from foreign FIUs in 2005. Thailand became a member of the Asia/Pacific Group on Money Laundering (APG), a FATF-style regional body, in April 2001. The AMLO joined the FATF's Egmont Group of financial intelligence units in June 2001.

The Government of Thailand should continue to implement its anti-money laundering program. The money laundering law should be amended to include the minimum list of acceptable designated categories of offenses prescribed by FATF and to make the "structuring" of transactions an offense. While the AMLA already captures proceeds of crime, it should be amended to include instrumentalities of offenses. Nonbank financial institutions and businesses such as gold shops, jewelry stores and car dealers should be subject to suspicious transaction reporting requirement without regard to a threshold. The insurance and securities sectors should institute AML compliance programs. AMLO should undertake audits of financial institutions to ensure compliance with requirements of AMLA and AMLO regulations. Until the RTG provides a viable mechanism for all of its financial institutions to be examined for compliance with the AMLA, Thailand's anti-money laundering regime will not comport with international standards.

The RTG should develop and implement anti-money laundering regulations for exchange businesses and should take additional measures to address the vulnerabilities presented by its alternative

remittance systems. The RTG can further strengthen its anti-money laundering regime by promulgating cross border currency control regulations that are currently pending in the Office of Secretary of the Cabinet. Thailand should ratify the UN Convention against Transnational Organized Crime and the UN Convention Against Corruption. Thailand should also immediately rescind its rewards program for AMLO investigators who seize assets under the anti-money laundering laws, and for agents of other law enforcement agencies that engage in similar reward schemes, as it gives the appearance of impropriety, can imperil successful prosecutions, and will eventually impede international cooperation and undermine public support for Thailand's forfeiture regime and its credibility. The current "interim" government has declared that it will limit itself to a term of around one year (i.e. until September 2007) and focus on drafting a new constitution. Its willingness and ability to pass new anti-money laundering laws and regulations are, therefore, extremely constrained.

Turkey

Turkey is an important regional financial center, particularly for Central Asia and the Caucasus, as well as for the Middle East and Eastern Europe. It continues to be a major transit route for Southwest Asian opiates moving to Europe. However, local narcotics trafficking organizations are reportedly responsible for only a small portion of the total funds laundered in Turkey.

Money laundering takes place in banks, nonbank financial institutions, and the underground economy. Money laundering methods in Turkey include: the cross-border smuggling of currency; bank transfers into and out of the country; trade fraud, and the purchase of high value items such as real estate, gold, and luxury automobiles. It is believed that Turkish-based traffickers transfer money and sometimes gold via couriers, the underground banking system, and bank transfers to pay narcotics suppliers in Pakistan or Afghanistan. Funds are often transferred to accounts in the United Arab Emirates, Pakistan, and other Middle Eastern countries. A substantial percentage of money laundering that takes place in Turkey involves fraud and tax evasion. Informed observers estimate that as much as 50 percent of the economy is unregistered. In 2005, the Government of Turkey (GOT) passed a tax administration reform law, with the goal of improving tax collection.

Turkey first criminalized money laundering in 1996. Under the law whoever commits a money laundering offense faces a sentence of two to five years in prison, and is subject to a fine of double the amount of the money laundered and asset forfeiture provisions. The Council of Ministers subsequently passed a set of regulations that require the filing of suspicious transaction reports (STRs), customer identification, and the maintenance of transaction records for five years.

In 2004, the GOT enacted additional anti-money laundering legislation, a new criminal law, and a new criminal procedures law. The new Criminal Law, which took effect in June 2005, broadly defines money laundering to include all predicate offenses punishable by one year's imprisonment. Previously, Turkey's anti-money laundering law comprised a list of specific predicate offenses. A new Criminal Procedures Law also came into effect in June 2005.

Under a Ministry of Finance banking regulation circular all banks, including the Central Bank, securities companies, post office banks, and Islamic financial houses are required to record tax identity information for all customers opening new accounts, applying for checkbooks, or cashing checks. The circular also requires exchange offices to sign contracts with their clients. The Ministry of Finance also mandates that a tax identity number be used in all financial transactions. The requirements are intended to increase the GOT's ability to track suspicious financial transactions. Turkey does not have bank secrecy laws that prevent disclosure of client and ownership information to bank supervisors and law enforcement officials. According to anti-money laundering law Article 5, public institutions, individuals, and corporate bodies must submit information and documents as well as adequate supporting information upon the request of Turkey's Financial Crimes investigation Board (MASAK) or other authorities specified in Article 3 of the law. Individuals and corporate bodies from whom

information and documents are requested may not withhold the requested items by claiming the protection provided by privacy provisions in order to avoid submitting the requested items.

A new Banking Law was enacted in 2005 to strengthen bank supervision. The Banking Regulatory and Supervisory Agency (BRSA) conducts periodic anti-money laundering and compliance reviews under the authority delegated by MASAK. The number of STRs currently being filed is quite low, even taking into consideration the fact that many commercial transactions are conducted in cash. In 2005, 352 STRs were filed, up from 288 in 2004 and 177 in 2003. The 2006 statistics are not available.

Turkey does not have foreign exchange restrictions. With limited exceptions, banks and special finance institutions must inform authorities within 30 days, about transfers abroad exceeding $50,000 (approximately 71,300 Turkish new liras) or its equivalent in foreign currency notes (including transfers from foreign exchange deposits). Travelers may take up to $5,000 (approximately 7,130 Turkish new liras) or its equivalent in foreign currency notes out of the country. Turkey does have cross-border currency reporting requirements. Article 16 of the recently-enacted MASAK law (see below) gives customs officials the authority to sequester valuables of travelers who make false or misleading declarations and imposes fines for such declarations.

MASAK was established by the 1996 anti-money laundering law as part of the Ministry of Finance. MASAK became operational in 1997, and it serves as Turkey's Financial Intelligence Unit (FIU), receiving, analyzing, and referring STRs for investigation. MASAK has three functions: regulatory, financial intelligence, and investigative. MASAK plays a pivotal role between the financial community and Turkish law enforcement, investigators, and judiciary.

In October 2006, Parliament enacted a new law reorganizing MASAK along functional lines, explicitly criminalizing the financing of terrorism, and providing safe harbor protection to the filers of STRs. The law also expands the range of entities subject to reporting requirements, to include art dealers, insurance companies, lotteries, vehicle sales outlets, antique dealers, pension funds, exchange houses, jewelry stores, notaries, sports clubs, and real estate companies. It also specifies sanctions for failure to comply. The law gives MASAK the authority to instruct a number of different inspection bodies (such as the bank examiners, the financial inspectors or the tax inspectors) to initiate an investigation if MASAK has reason to suspect financial crimes. Likewise, MASAK can refer suspicious cases to the Public Prosecutor and the Public Prosecutor can ask MASAK to conduct a preliminary investigation prior to referring a case to the police for criminal investigation.

However, neither the current draft of the legislation, nor a June 2006 set of amendments to Turkey's antiterrorism laws, expanded upon Turkey's narrow definition of terrorism applicable only in terms of attacks on Turkish nationals or the Turkish state.

According to MASAK statistics, as of December 31, 2005 it had pursued 2,231 money laundering investigations since its 1996 inception, but fewer than ten cases resulted in convictions. Moreover, all of the convictions are reportedly under appeal. Most of the cases involve nonnarcotics criminal actions or tax evasion; as of December 31, 2005 41 percent of the cases referred to prosecutors were narcotics-related.

The GOT enforces existing drug-related asset seizures and forfeiture laws. MASAK, the Turkish National Police, and the courts are the government entities responsible for tracing, seizing and freezing assets. According to Article 9 of the anti-money laundering law, the Court of Peace—a minor arbitration court for petty offenses—has the authority to issue an order to freeze funds held in banks and nonbank financial institutions as well as other assets, and to hold the assets in custody during the preliminary investigation. During the trial phase, the presiding court has freezing authority. Public Prosecutors may freeze assets in cases where it is necessary to avoid delay. The Public Prosecutors' Office notifies the Court of Peace about the decision within 24 hours. The Court of Peace has 24 hours

to decide whether to approve the action. There is no time limit on freezes. There is no provision in Turkish law for the sharing of seized assets with other countries.

MASAK's General Communiqué No. 3, requires that a special type of STR be filed by financial institutions in cases of suspected terrorist financing. However, until the amendments to the criminal code were enacted in June 2006, terrorist financing was not explicitly defined as a criminal offense under Turkish law. Various existing laws with provisions that can be used to punish the financing of terrorism include articles 220, 314 and 315 of the Turkish penal code, which prohibit assistance in any form to a criminal organization or to any organization that acts to influence public services, media, proceedings of bids, concessions, and licenses, or to gain votes, by using or threatening violence. To commit crimes by implicitly or explicitly intimidating people is illegal under the provisions of the Law No. 4422 on the Prevention of Benefit-Oriented Criminal Organizations. The GOT distributes to GOT agencies and financial institutions the names of suspected terrorists and terrorist organizations on the UNSCR 1267 Sanctions Committee consolidated list, as well as U.S.-designated names.

Another area of vulnerability in the area of terrorist financing is the GOT's supervision of nonprofit organizations. The General Director of Foundations (GDF) issues licenses for charitable foundations and oversees them. The Ministry of Interior regulates charitable nongovernmental associations (NGOs). Both the GDF and the Ministry of Interior keep central registries of the charitable organizations they regulate and they require charities to verify and prove their funding sources and to have bylaws. Charitable foundations are audited by the GDF and are subject to being shut down if they act outside the bylaws. Charitable organizations are required to submit periodic financial reports to the regulators. The regulators and the police closely monitor monies received from outside Turkey. The police also monitor NGO's for links to terrorist groups.

Alternative remittance systems are illegal in Turkey, and in theory only banks and authorized money transfer companies are permitted to transfer funds. Trade-based money laundering, fraud, and underground value transfer systems are also used to avoid taxes and government scrutiny. There are 21 free trade zones operating in Turkey. The GOT closely controls access to the free trade zones. Turkey is not an offshore financial center.

According to MASAK statistics, no assets linked to terrorist organizations or terrorist activities were frozen in 2005. Turkey has a system for identifying, tracing, freezing, and seizing assets that are not related to terrorism, although the law allows only for their criminal forfeiture and not their administrative forfeiture. Article 7 of the anti-money laundering law provides for the confiscation of all property and assets (including derived income or returns) that are the proceeds of a money laundering predicate offense (soon to be expanded to crimes punishable by one year imprisonment), once the defendant is convicted. The law allows for the confiscation of the equivalent value of direct proceeds that could not be seized. Instrumentalities of money laundering can be confiscated under the law. In addition to the anti-money laundering law, Articles 54 and 55 of the Criminal Code provide for post-conviction seizure and confiscation of the proceeds of crimes. The defendant, however, must own the property subject to forfeiture. Legitimate businesses can be seized if used to launder drug money or support terrorist activity, or are related to other criminal proceeds. Property or its value that is confiscated is transferred to the Treasury.

The Council of Ministers promulgated a decree (2482/2001) to freeze all the funds and financial assets of individuals and organizations included on the UNSCR 1267 Sanctions Committee's consolidated list. However, the tools currently available under Turkish law for locating, freezing, seizing and confiscating terrorist assets are cumbersome, limited and not particularly effective. For example, there is no legal mechanism to freeze the assets of terrorists not on the UN consolidated list. Even for names on the list, Turkey's decree-based system of freezing 1267-listed names was challenged in court. In July 2006, a chamber of the Council of State (administrative court) ruled that the GOT lacked the

authority to freeze assets by decree since property rights are protected under the Turkish constitution. The assets of the 1267-listed individual continue to be frozen and this ruling is under appeal.

The GOT cooperates closely with the United States and with its neighbors in the Southeast Europe Cooperation Initiative (SECI). Turkey and the United States have a Mutual Legal Assistance Treaty (MLAT) and cooperate closely on narcotics and money laundering investigations. Turkey is a member of the Financial Action Task Force (FATF). MASAK is a member of the Egmont Group. Turkey is a party to the 1988 UN Drug Convention, the UN International Convention for Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. Turkey has signed and ratified the COE Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds of Crime, which came into force on February 1, 2005. In 2006, Turkey became a party to the UN Convention against Corruption.

With the passage of several new pieces of legislation, the Government of Turkey took steps in 2005 and 2006 to strengthen its anti-money laundering and counterterrorist financing regime. It now faces the challenge of aggressively implementing these laws. Turkey should improve its coordination among the various entities charged with responsibility in its anti-money laundering and counterterrorist financing regime, including the various courts with responsibilities for these issues, in order to increase the number of successful investigations and prosecutions. Turkey should also regulate and investigate alternative remittance networks to thwart their potential misuse by terrorist organizations or their supporters. Turkey should consider expanding its narrow legal definition of terrorism. Turkey should continue tax reform that will help minimize the underground economy. It should also strengthen its oversight of charities.

Turks and Caicos

The Turks and Caicos Islands (TCI) is a Caribbean overseas territory of the United Kingdom (UK). The TCI is comprised of two island groups and forms the southeastern end of the Bahamas archipelago. The U.S. dollar is the currency in use. The TCI has a significant offshore center, particularly with regard to insurance and international business companies (IBCs). Its location has made it a transshipment point for narcotics traffickers. The TCI is vulnerable to money laundering because of its large offshore financial services sector, as well as its bank and corporate secrecy laws and internet gaming activities. As of 2006, the TCI's offshore sector has eight banks, four of which also offer offshore banking; approximately 2,500 insurance companies; 20 trusts; and 17,000 "exempt companies" that are IBCs.

The Financial Services Commission (FSC) licenses and supervises banks, trusts, insurance companies, and company managers. It also licenses IBCs and acts as the Company Registry for the TCI. These institutions are subject to on-site examination to determine compliance with TCI laws and regulations. In 2006, the Financial Services Commission employed a staff of 21, including four regulators. The FSC became a statutory body under the Financial Services Commission Ordinance 2001 and became operational in March 2002. It now reports directly to the Governor, as well as the Minister of Finance. The FSC is in the process of adopting a risk-based examination approach to better assess, identify, measure, monitor and control threats associated with potential money laundering and terrorist financing.

The offshore sector offers "shelf company" IBCs, and all IBCs are permitted to issue bearer shares. However, the Companies (Amendment) Ordinance 2001 requires that bearer shares be immobilized by depositing them, along with information on the share owners, with a defined licensed custodian. This applies to all shares issued after enactment and allows for a phase-in period for existing bearer shares of two years. Trust legislation allows establishment of asset protection trusts inoculating assets from civil adjudication by foreign governments; however, the Superintendent of Trustees has investigative

powers and may assist overseas regulators. Currently, the FSC is rewriting the trust legislation with assistance from the UK Government.

The 1998 Proceeds of Crime Ordinance (PCO) criminalizes money laundering related to all crimes and provides "safe harbor" protection for good faith compliance with reporting requirements. The PCO allows for the criminal forfeiture of assets related to money laundering and other offenses, although civil forfeiture is not permitted. The PCO also establishes a Money Laundering Reporting Authority (MLRA), chaired by the Attorney General, to receive, analyze and disseminate financial disclosures such as suspicious activity reports (SARs). Its members also include the following individuals or their designees: Collector of Customs, the Managing Director of the FSC and the Head of its Financial Crimes Unit (FSU), the Superintendent of the FSC, the Commissioner of Police, and the Superintendent of the Criminal Investigation Department. The MLRA is authorized to disclose information it receives to domestic law enforcement and foreign governments.

The Proceeds of Crime (Money Laundering) Regulations came into force January 14, 2000. The Money Laundering Regulations place additional requirements on the financial sector such as identification of customers, retention of records for a minimum of ten years, training staff on money laundering prevention and detection, and development of internal procedures in order to ensure proper reporting of suspicious transactions. The Money Laundering Regulations apply to banks, insurance companies, trusts, mutual funds, money remitters, investment dealers and issuers of credit cards. However, money remitters and investment dealers have no supervisory or regulatory authority to oversee compliance with the regulations. Other sectors, such as gambling, jewelers, real estate companies and currency exchange companies, are not subject to the Money Laundering Regulations. Although the customer identification requirements only apply to accounts opened after the Regulations came into force, TCI officials have indicated that banks would be required to conduct due diligence on previously existing accounts by December 2005.

In 1999, the FSC, acting as the secretary for the MLRA, issued nonstatutory Guidance Notes to the financial sector, in order to help educate the industry regarding money laundering and the TCI's anti-money laundering requirements. Additionally, it provided practical guidance on recognizing suspicious transactions. The Guidance Notes instruct institutions to send SARs to either the Royal Turks & Caicos Police Force or the FSC. Officials forward all SARs to the Financial Crimes Unit (FCU) of the Royal Turks and Caicos Islands Police Force, which analyzes and investigates financial disclosures. The FCU also acts as the TCI's financial intelligence unit (FIU).

As with the other United Kingdom Caribbean overseas territories, the Turks and Caicos underwent an evaluation of its financial regulations in 2000, co-sponsored by the local and British governments. The report noted several deficiencies and the government has moved to address most of them. The report noted the need for improved supervision, which the government acknowledged. An Amendment to the Banking Ordinance was introduced in February 2002 to remedy deficiencies outlined in the report relating to notification of the changes of beneficial owners, and increased access of bank records to the FSC. However, legislation has not been introduced to remedy the deficiencies noted in the report with respect to the Superintendent's lack of access to the client files of Company Service and Trust providers, nor is there legislation that clarifies how the internet gaming sector is to be supervised with respect to anti-money laundering compliance.

As a UK territory, the TCI is subject to the United Kingdom Terrorism (United Nations Measure) (Overseas Territories) Order 2001. However, the Government of the TCI has not yet implemented domestic orders that would criminalize the financing of terrorism. The UK's ratification of the International Convention for the Suppression of the Financing of Terrorism has not been extended to the TCI.

The TCI cooperates with foreign governments—in particular, the United States and Canada—on law enforcement issues, including narcotics trafficking and money laundering. The FCU also shares

information with other law enforcement and regulatory authorities inside and outside of the TCI. The Overseas Regulatory Authority (Assistance) Ordinance 2001, allows the TCI to further assist foreign regulatory agencies. This assistance includes search and seizure powers and the power to compel the production of documents.

The TCI is a member of the Caribbean Financial Action Task Force, and is subject to the 1988 UN Drug Convention. The Mutual Legal Assistance Treaty between the United States and the United Kingdom concerning the Cayman Islands was extended to the TCI in November 1990.

The Government of the Turks and Caicos Islands has put in place a comprehensive system to combat money laundering with the relevant legislative framework. The FSC has made steady progress in developing its regulatory capability and has some experienced senior staff. Notwithstanding, the current regulatory structure is not fully in accordance with international standards. The Turks and Caicos Islands should extend existing regulations to all sectors, bring all obligated entities under the supervision of a regulatory body, and enhance its on-site supervision program. The Turks and Caicos Islands should take the necessary steps to ensure that its FIU is eligible for membership in the Egmont Group of financial intelligence units. The Government of the TCI should criminalize the financing of terrorists and terrorism. Turks and Caicos Islands should expand efforts to cooperate with foreign law enforcement and administrative authorities. Turks and Caicos Islands should also provide adequate resources and authorities to provide supervisory oversight of its offshore sector in order to further ensure criminal or terrorist organizations do not abuse the Turks and Caicos Islands' financial sector.

Ukraine

Corruption, organized crime, prostitution, smuggling, tax evasion, trafficking in persons, drugs and arms, and other organized criminal activity continue to be sources of laundered funds in Ukraine. As of June 30, 2006, Ukraine has approximately 160 active banks, two of which are state-owned. There are no offshore financial centers or facilities under Ukraine's jurisdiction.

In January 2001, the Government of Ukraine (GOU) enacted the "Act on Banks and Banking Activities," which imposes some anti-money laundering (AML) requirements upon banking institutions. The Act prohibits banks from opening accounts for anonymous persons, requires the reporting of large transactions and suspicious transactions to state authorities, and provides for the lifting of bank secrecy pursuant to an order of a court, prosecutor, or specific state body. In August 2001, the President signed the "Law on Financial Services and State Regulation of the Market of Financial Services." This law establishes regulatory control over nonbank financial institutions that manage insurance, pension accounts, financial loans, or "any other financial services involving savings and money from individuals." The law defines financial "institutions" and "services," imposes record keeping requirements on obligated entities, and identifies the responsibilities of regulatory agencies. The law established the State Commission on Regulation of Financial Services Markets, which, along with the National Bank of Ukraine (NBU) and the State Commission on Securities and the Stock Exchange, has responsibility for regulating financial services markets.

When the Financial Action Task Force (FATF), placed Ukraine on the list of noncooperative countries and territories (NCCT) in September 2001, it noted that Ukraine lacked (1) a complete set of anti-money laundering (AML) laws, (2) an efficient mandatory system for reporting suspicious transactions to a Financial Intelligence Unit (FIU), (3) adequate customer identification requirements, and (4) adequate resources at present to combat money laundering. Following the FATF action, the U.S. Treasury Department issued an advisory to all U.S. financial institutions instructing them to "give enhanced scrutiny" to all transactions involving Ukraine.

On November 28, 2002, President Kuchma signed into law Ukrainian Law No. 249-IV, an anti-money laundering package entitled "On Prevention and Counteraction of the Legalization (Laundering) of the

Proceeds from Crime" (the Basic AML Law). The Basic AML Law establishes a two-tiered system of financial monitoring consisting of initial financial monitoring (i.e. obligated entities that carry out financial transactions) and state financial monitoring (i.e. government agencies charged with regulation and supervision of the financial institutions). Overall regulatory authority is vested in the State Committee for Financial Monitoring (SCFM), in accordance with Article 4 of the AML law.

In December 2002, the FATF determined that Ukraine's AML statute did not meet international standards and recommended that FATF members impose countermeasures on Ukraine. Under Section 311 of the USA PATRIOT Act, the United States designated Ukraine as a jurisdiction of primary money laundering concern. In December 2002 and February 2003, in response to the imminent threat of countermeasures, Ukraine passed further legislative amendments in accordance with FATF recommendations.

Legislation enacted in February 2003 requires banks and other financial service providers to implement AML compliance programs, conduct due diligence to identify beneficial account owners prior to allowing the opening an account or conducting certain transactions, report suspicious transactions to the SCFM and maintain records on suspicious transactions and the people carrying them out for a period of five years. The legislation includes a "safe harbor" provision that protects reporting institutions from liability for cooperating with law enforcement agencies. Immediately upon passage of the February amendments, the FATF withdrew its call for members to invoke countermeasures and the United States followed suit on April 17, 2003, by revoking Ukraine's designation under Section 311 of the USA PATRIOT Act as a jurisdiction of primary money laundering concern. In August 2003, the State Commission established the State Register of financial institutions, and by October 2006, the State Register contained information on 1375 nonbank financial institutions.

By passing comprehensive anti-money laundering legislation, Ukraine initiated the process of NCCT de-listing. At the FATF plenary in September 2003, Ukraine was invited to submit an implementation plan, and an on-site visit to assess Ukraine's progress in developing its AML regime was conducted on January 19-23, 2004. The positive results of the on-site visit by the FATF evaluation team were reported to the European Review Group (ERG), and Ukraine was removed from the NCCT list at the FATF plenary on February 25, 2004. As a condition of de-listing, Ukraine continued to undergo monitoring by the FATF on implementation of its AML regime. Since November 2004, the GOU has made several efforts to pass a set of amendments to the AML law in order to bring Ukraine's regime into compliance with FATF's revised Forty plus Nine recommendations. The Rada, or Parliament, twice rejected the government's draft in 2005. The government has redrafted the law, narrowing its scope to the FATF recommendations, and omitting provisions introducing new SCFM authority and other bureaucratic changes that had drawn opposition in the Parliament. Among other provisions, the new legislation would expand the sectors subject to primary monitoring to include retail traders, lawyers, accountants, and traders of precious metals. The law, entitled "On Amending Some Legislative Acts of Ukraine on Prevention to Legalization (Laundering) of the Proceeds from Crime and Terrorist Financing", was registered in the Verkhovna Rada on December 28, 2006. The bill was also referred to a special expert committee called the Main Scientific Expertise Department, which provided commentary, along with the recommendation that the Rada address some problems mainly regarding terminology, and then approve the bill on its first reading.

In 2004, authorities reduced the monetary threshold beyond which transactions and operations are subject to compulsory financial monitoring from Ukrainian Hryvnias (UAH) 300,000 (approximately $59,650) for cashless payments and UAH 100,000 (approximately $19,900) for cash payments, to UAH 80,000 (approximately $15,900) for payments using either method. The compulsory reporting threshold exists only if the transaction also meets one or more suspicious activity indicators as set forth in the law. Any transaction suspected of being connected to terrorist activity must be reported to the appropriate authorities immediately.

Beginning in August 2005, as a result of amendments to the "Resolution on the Adoption of Instructions Regarding Movement of Currency, Precious Metals, Payment Documents, and Other Banking Documents over the Customs Border of Ukraine," the law mandates that travelers declare cross-border transportation of cash sums exceeding $3,000. Cash smuggling is substantial in Ukraine, although it is reportedly related more to unauthorized capital flight rather than to criminal proceeds or terrorist funding.

In 2005, the GOU sought to combat smuggling and corruption by reducing import duties, introducing new procedures for the Customs Service, and implementing transparent procedures for the privatization of state enterprises. Ukraine's 2005 budget eliminated the tax and customs duty privileges available in eleven Free Economic Zones and nine Priority Development Territories that operated within Ukraine. However, in August 2006, the government announced its intention to restore tax and customs privileges for businesses operating in the SEZs beginning in 2007. Although legislation implementing this policy decision had not yet passed the Parliament by the end of 2006, the GOU asserts that the SEZs will avoid the problems of the past.

Ukraine enacted Law 3163-IV in January 2006; this law amended the initial AML laws. Under the new Law, the entities obligated to conduct initial financial monitoring must be able to provide proof that they are fulfilling all Know Your Customer (KYC) identification requirements. Ukraine also granted state agencies enhanced authority to exchange information internationally, improved rules on bank organization, and implemented a screening requirement at the level of financial institutions. On September 14, 2006, Ukraine enacted amendments to the "Law on Banks and Banking" that require all banks to be formed as open joint-stock companies or as cooperatives. This measure strengthens disclosure requirements on the identity of the beneficial owners of banks. These amendments apply to all newly formed banks and provide a three-year period for existing banks to comply. As a result of these and other improvements to its legal framework, in February 2006, the FATF suspended its direct monitoring of Ukraine, which had been in place since December 2002.

The Criminal Code of Ukraine has separate provisions criminalizing drug-related and nondrug-related money laundering. Amendments to the Code adopted in January 2003 included willful blindness provisions and expanded the scope of predicate crimes for money laundering to include any action punishable under the Criminal Code with imprisonment of three years or more, excluding certain specified actions.

The SCFM is Ukraine's financial intelligence unit (FIU). The December 10, 2001 Presidential Decree "Concerning the Establishment of a Financial Monitoring Department" mandated the establishment of the SCFM as Ukraine's FIU. The SCFM became operational on June 12, 2003. At that time, the SCFM was an independent authority administratively subordinate to the Ministry of Finance and the sole agency authorized to receive and analyze financial information from financial institutions. On March 18, 2004, Ukraine's Rada granted the SCFM the status of a central executive agency, subordinate to the Cabinet of Ministers rather than to the Ministry of Finance. This change became effective on January 1, 2005. As of October 1, 2006, the SCFM had established 21 local branches in Ukraine's regions.

The SCFM is an administrative agency with no investigative or arrest authority. It is authorized to collect suspicious transaction reports and analyze suspicious transactions, including those related to terrorist financing, and to transfer financial intelligence information to competent law enforcement authorities for investigation. The SCFM also has the authority to conclude interagency agreements and exchange intelligence on financial transactions involving money laundering or terrorist financing with other FIUs. As of October 2006, the SCFM had concluded memoranda of understanding (MOUs) with the FIUs of thirty countries, and was working on fourteen additional MOUs.

The SCFM has processed, analyzed, and developed cases reportedly to the point of establishing the equivalent of probable cause prior to referral to law enforcement. It has become a regional leader with

regard to the volume of case information exchanged with counterpart FIUs. The SCFM acknowledges the existence and use of alternative remittance systems in Ukraine, and its personnel have attended seminars and exchanged information about such systems. The SCFM and security agencies monitor charitable organizations and other nonprofit entities that might be used to finance terrorism.

In 2005, the SCFM received 786,251 transaction reports, which include STRs and automatic threshold reports. The majority of these were submitted by banks. The SCFM designated approximately 11 percent of these for "active research" and sent 321 separate cases to law enforcement agencies. From January to November 2006, the SCFM received a total of 692,280 transaction reports. Over that same period, the SCFM referred 31 cases to the Prosecutor General's Office, 115 cases to the State Tax Administration, 127 cases to the Ministry for Internal Affairs, and 154 cases to the State Security Service of Ukraine. As a result of subsequent investigation of these 427 cases, law enforcement agencies initiated 161 criminal cases. Of these, prosecutors brought 8 cases to trial, with one conviction.

Although the reporting system is effective and the SCFM has generated a substantial number of cases, law enforcement authorities and prosecutors did not succeed in obtaining a large number of convictions. Observers reportedly believe the key problem to be local prosecutors who close money laundering investigations and cases prematurely or arbitrarily, possibly because of corruption and possibly because of a weak understanding of money laundering crimes on the part of authorities—for example, authorities are inclined to include tax crimes as money laundering. Ukraine has been working with the European Commission and Council of Europe to increase its capacity to fight money laundering and terrorism financing. The first such undertaking took place from 2003-2005 and was called "Project Against Money Laundering in Ukraine," or MOLA-UA. Those involved decided it was so successful that in September 2006, a follow-up "Project Against Money Laundering and Terrorist Financing in Ukraine" (MOLA-UA2) was established, with a focus on education, training and cooperation. MOLA-UA2 will run through April 2009 and focus on three areas: getting Ukraine's legislative framework up to international standards; enhancing the human capacities of key institutions and agencies; and developing the organizational and technical infrastructure of the system.

Ukraine has an asset forfeiture regime. Article 59 of the Ukrainian Criminal Code provides for the forceful seizure of all or a part of the property of a person convicted for grave and especially grave offenses as set forth in the relevant part of the code. With respect to money laundering, Article 209 allows for the forfeiture of criminally obtained money and other property.

On December 10, 2003, the Cabinet of Ministers issued Decree No. 1896, establishing a Unified State Information System of Prevention and Counteraction of Money Laundering and Terrorism Financing. Through this system, fourteen ministries and agencies share information by providing each other with monthly database updates. The Government is planning to automate this information sharing in 2007 by establishing a secure electronic network linking these agencies.

Law 3163-IV, which entered into force on January 1, 2006, enhanced Ukraine's ability to exchange information internationally and placed greater obligations on banks to combat terrorist financing. This Law requires banks to adopt procedures to screen parties to all transactions using a SCFM-issued list of beneficiaries of, or parties to, terrorist financing. Banks must freeze assets for two days and immediately inform the FIU and law enforcement bodies whenever a party to a transaction appears on the list. The FIU can extend the freeze to five days. During the first half of the year, banks developed their screening capabilities. On October 25, 2006, the Cabinet of Ministers approved the SCFM's list, drawn from three sources: the United Nations 1267 Sanctions Committee's consolidated list, information from the Ukrainian Security Service on individuals and entities suspected of violating article 258 of the Ukrainian Criminal Code concerning terrorism, and the lists compiled by those countries that have bilateral agreements with Ukraine on mutual recognition of terrorist designations. On September 21, 2006, the Rada enacted revisions to Article 258 of the Criminal Code, adding

Article 258-4 which explicitly criminalizes terrorist financing. The revised text mandates imprisonment from three to eight years for financing, material provision, or provision of arms with the aim of supporting terrorism. The revisions also amend the criminal procedure code to empower the State Security Service (SBU) with primary responsibility for investigation of terrorist financing.

The GOU has cooperated with U.S. efforts to track and freeze the financial assets of terrorists and terrorist organizations. The NBU, the State Commission for the Regulation of Financial Services, the Securities Exchange Commission, the State Tax Administration, the SBU, and the Ministries of Finance, Internal Affairs, and Foreign Affairs are informed about the U.S.-designation of suspected terrorists and terrorist organizations under E.O. 13224 and other U.S. authorities. Through their regulatory agencies, banks and nonbank financial services also receive these U.S.-designations, and are instructed to report any transactions involving designated individuals or entities.

The U.S.-Ukraine Treaty on Mutual Legal Assistance in Criminal Matters was signed in 1998 and entered into force in February 2001. A bilateral Convention for the Avoidance of Double Taxation and the Prevention of Fiscal Evasion with Respect to Taxes on Income and Capital, which provides for the exchange of information in administrative, civil, and criminal matters, is also in force.

Ukraine is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. Ukraine is a signatory to the UN Convention against Corruption. Ukraine is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), a FATF-style regional body (FSRB). It is also an observer and technical assistance donor to the Eurasian Group on Combating Money Laundering and the Financing of Terrorism (EAG), another FSRB. The SCFM is a member of the Egmont Group.

Ukraine has strengthened and clarified its newly adopted laws. With the SCFM, the NBU, and other actors in the financial and legal sectors, Ukraine has established a comprehensive AML regime. To date, however, Ukraine's ability to implement this regime through consistent successful criminal prosecutions has yet to be proven. The Prosecutor General's office should address the deficiencies of that office, such as limited professional experience with money laundering among staff, which can result in prosecutors' limited commitment to criminal prosecution. The GOU should take action to establish oversight capabilities of local investigators, prosecutors, and judges to insure that cases are vigorously pursued and prosecuted. Law enforcement agencies should give higher priority to investigating money laundering cases. Both law enforcement officers and the judiciary need a better understanding of the theoretical and practical aspects of investigating and prosecuting money laundering cases. Ukraine should become a party to the UN Convention against Corruption and prosecute and convict corrupt public officials.

United Arab Emirates

The United Arab Emirates (UAE) is an important financial center in the Persian Gulf region. Although the financial sector is modern and progressive, the UAE remains a largely cash-based society. Dubai, in particular is a major international banking center. The country also has a growing offshore sector. The UAE's robust economic development, political stability, and liberal business environment have attracted a massive influx of people, goods, and capital. The UAE is particularly susceptible to money laundering due to its geographic location as the primary transportation and trading hub for the Gulf States, East Africa, and South Asia; and its expanding trade ties with the countries of the former Soviet Union and lack of transparency in its corporate environment. The potential for money laundering is exacerbated by the large number of resident expatriates (roughly 80 percent of total population) from the aforementioned regions to the UAE who send remittances to their homelands. Given the country's proximity to Afghanistan, where most of the world's opium is produced, narcotics traffickers are increasingly reported to be attracted to the UAE's financial and trade centers. Other

sources of money laundering in the UAE include hawala, trade fraud, the real estate boom, the misuse of the international gold trade, conflict diamonds and smuggling.

Following the September 11, 2001 terrorist attacks in the United States, and amid revelations that terrorists had moved funds through the UAE, the Emirates' authorities acted swiftly to address potential vulnerabilities. In close concert with the United States, the UAE imposed a freeze on the funds of groups with terrorist links, including the Al-Barakat organization, which was headquartered in Dubai. Both national and emirate-level officials have gone on record as recognizing the threat money laundering activities in the UAE pose to the nation's reputation and security. Since 2001, the UAE Government (UAEG) has taken steps to better monitor cash flows through the UAE financial system and to cooperate with international efforts to combat terrorist financing. The UAE has enacted the Anti-Money Laundering Law No. 4/2002, and the Anti-Terrorism Law No. 1/2004. Both pieces of legislation, in addition to the Cyber Crimes Law No. 2/2006, serve as the foundation for the country's anti-money laundering and counterterrorist financing efforts.

Law No. 4 of 2002 criminalizes all forms of money laundering activities. The law calls for stringent reporting requirements for wire transfers exceeding 2000 dirhams (approximately $545) and currency imports above 40,000 dirhams (approximately $10,900).The law imposes stiff criminal penalties for money laundering that includes up to seven years in prison plus a fine of up to 300,000 dirhams (approximately $81,700), as well as a seizure of assets upon conviction. The law also provides safe harbor provisions for reporting officers.

Prior to the passage of the Anti-Money Laundering Law, the National Anti-Money Laundering Committee (NAMLC) was established in July 2000 to coordinate the UAE's anti-money laundering policy. The NAMLC was later codified as a legal entity by Law No. 4/2002, and is chaired by the Governor of the Central Bank. Members of the NAMLC include representatives from the Ministries of Interior, Justice, Finance, and Economy, the National Customs Board, Secretary General of the Municipalities, Federation of the Chambers of Commerce, and five major banks and money exchange houses (as observers).

Administrative Regulation No. 24/2000 provides guidelines to financial institutions for monitoring money laundering activity. This regulation requires banks, money exchange houses, finance companies, and any other financial institutions operating in the UAE to follow strict know your customer guidelines. Financial institutions must verify the customer's identity and maintain transaction details (i.e., name and address of originator and beneficiary) for all exchange house transactions over $545 and for all non-account holder bank transactions over $10,900. The regulation delineates the procedures to be followed for the identification of natural and juridical persons, the types of documents to be presented, and rules on what customer records must be maintained on file at the institution. Other provisions of Regulation 24/2000 call for customer records to be maintained for a minimum of five years and further require that they be periodically updated as long as the account is open.

In July, 2004, the UAE government strengthened its legal authority to combat terrorism and terrorist financing by passing Federal Law Number No. 1/2004. The Law specifically criminalizes the funding of terrorist activities and terrorist organizations. It sets stiff penalties for the crimes covered, including life imprisonment and the death penalty. It also provides for asset seizure or forfeiture. Under the law, founders of terrorist organizations face up to life imprisonment. The law also penalizes the illegal manufacture, import, or transport of "nonconventional weapons" and their components that are intended for use in a terrorist activity.

Article 12 provides that raising or transferring money with the "aim or with the knowledge" that some or all of this money will be used to fund terrorist acts is punishable by "life or temporary imprisonment," regardless if these acts occur. Law No. 1/2004 grants the Attorney General (or his deputies) the authority to order the review of information related to the accounts, assets, deposits,

transfer, or property movements on which the Attorney General has "sufficient evidence to believe" are related to the funding or committing of a terror activity stated in the law.

The law also provides for asset seizure and confiscation. Article 31 gives the Attorney General the authority to seize or freeze assets until the investigation is completed. Article 32 confirms the Central Bank's authority to freeze accounts for up to seven days if it suspects that the funds will be used to fund or commit any of the crimes listed in the law. The law also allows the right of appeal to "the competent court" of any asset freeze under the law. The court will rule on the complaint within 14 days of receiving the complaint. Through 2005, there were no reported criminal convictions for money laundering or terrorist financing under either the 2002 or the 2004 laws.

Law No. 1/2004 also established the "National Anti-Terror Committee" (NATC) to serve as the government's interagency liaison with respect to implementing the United Nations Security Council Resolutions on terrorism, and sharing information with its foreign counterparts as well as with the United Nations. Representatives from Ministries of Foreign Affairs, Interior, Justice, and Defense; Central Bank; State Security Department; and Federal Customs Authority comprise the NATC

The Anti-Money Laundering and Suspicious Case Unit (AMLSCU) was established in 2002 as the UAE's financial intelligence unit (FIU), and was housed within the Central Bank. In addition to receiving Suspicious Transaction Reports, the AMLSCU is authorized to send and receive information requests from foreign regulatory authorities in order to conduct its preliminary investigations based on suspicious transaction report data. The AMLSCU joined the Egmont Group in June 2002, and has regularly exchanged information with foreign FIUs on a reciprocal basis. It has also provided information by request to foreign FIUs (including the United States) regarding investigations being conducted in other countries. As of October 2006, the AMLSCU has received and investigated a total of 3954 suspicious transactions reports (STRs), 829 of which were received between December 2005 and October 2006. Based on AMLSCU and law enforcement investigations from these STRs, a total of 27 freeze orders were issued by the Central Bank between December 2000 (prior to the establishment of the FIU) and October 2006, one of which was issued in 2006. Of these 27 cases of freeze orders, 9 cases are currently in the process of prosecution for money laundering and confiscation of criminal proceeds. The Central Bank also ensures that it circulates an updated UNSCR 1267 Sanctions Committee's consolidated list of suspected terrorists and terrorist organizations to all the financial institutions under its supervision. Since 2000, the Central Bank has frozen a total of $1,348,381 from 17 separate bank accounts based on the names contained in the UNSCR 1267 list.

Several amendments were made to the Central Bank Regulations 24/2000 in July 2006. First, the regulations added the term "terrorism financing" to any references made to the term "money laundering." Second, the Regulations required financial institutions to freeze transactions that they believe may be destined for funding terrorism, terrorist organizations, or for terrorist purposes. The Regulations also require financial institutions to notify the financial intelligence unit (FIU) in writing of such transactions "in case of any doubt". Finally, the enhanced due diligence requirements for charities were made requiring banks to obtain a certificate from the Minister of Social Affairs before opening or maintaining any charitable organization-type account.

In 2006, the UAE enacted Law No. 2/2006 of the Cyber Crimes. Article 19 of the law criminalized the electronic transfer of money or property through the internet in which the true sources of such assets are either concealed or linked to criminal proceeds. Violations are punishable by up to seven years imprisonment and fines ranging from approximately $8,170 to $54,500. Article 21 of the law outlaws the use of the internet to finance terrorist activities, promote terrorist ideology, disseminate information on explosives, or to facilitate contact with terrorist leaders. Any violation of Article 21 is punishable by up to 5 years imprisonment.

The Central Bank is responsible for supervising the UAE financial sectors, which include banks, exchange houses, and investment companies. It is authorized to issue licenses and impose

administrative sanctions for compliance violations. The Central Bank also has the authority to issue instructions and recommendations to financial institutions as it deems appropriate, and to take any measures as necessary to ensure the integrity of the UAE's financial system

Some money laundering in the UAE is known to occur through the numerous money exchange houses. However, hawala is where money laundering activity is likely more prevalent due to the largely undocumented nature of this informal remittance system. Dubai is a regional hawala center. Hawala is an attractive mechanism for terrorist and criminal exploitation due to the nontransparent and highly resilient nature of the system to law enforcement and regulators. In 2002, the Central Bank issued new regulations to help improve the oversight of hawala. The new regulations required hawala brokers (hawaladars) to register with the Central Bank, submit the names and addresses of all originators and beneficiaries of funds, and to file suspicious transaction reports on a monthly or quarterly basis. However, since the inception of the program, there reportedly have not been any suspicious reports filed by hawaladars.

As of November 30, 2006, the Central Bank issued 201 licenses to hawaladars, with an additional 38 applicants currently working to complete their licensing requirements. Once issued a formal license, the Central Bank conducts one-on-one training sessions with each registered hawaladar to ensure that dealers understand the record-keeping and reporting obligations. The registered hawaladars are also required to use an account they open at the Central Bank to process their transactions. Currently, there is no accurate estimate of the total number of UAE-based hawala brokers, and there is no penalty for failure of hawaladars to register with the Central Bank. The UAE has hosted three international Conferences on hawala, and plans to host a fourth in March 2007.

The UAE has not set any limits on the amount of cash that can be imported into or exported from the country. No reporting requirements exist for cash exports. However, the Central Bank requires that any cash imports over $10,900 must be declared to Customs; otherwise undeclared cash may be seized upon attempted entry into the country. Upon seizing any undeclared cash, UAE authorities have the jurisdiction to conduct an investigation into the source of these funds. All cash forfeiture cases are handled at the judicial level because there are no administrative procedures to handle forfeited cash. Since the UAE is a cash-based economy, it is not unusual for people to carry significant sums of cash in general. As a result, customs officials, police, and judicial authorities tend to not regard large cash imports as potentially suspicious or criminal type activities.

The UAE authorities have admitted the need to better regulate "near-cash" items such as gold, jewelry, and gemstones, especially in the burgeoning markets located in Dubai. The UAE has participated in the Kimberley Process Certification Scheme for Rough Diamonds (KPCS) since November 2002, and began certifying rough diamonds exported from the UAE on January 1, 2003. In 2004, the UAE was the first KPCS participant country to volunteer for a "peer review visit" on internal control mechanisms. The Dubai Metals and Commodities Center (DMCC) is a quasi-governmental organization charged with issuing Kimberly Process (KP) certificates in the UAE, and employs four full-time individuals to administer the KP program. Prior to January 1, 2003, the DMCC circulated a sample UAE certificate to all KP member states and embarked on a public relations campaign to educate the estimated 50 diamond traders operating in Dubai with the new KP requirements. Under the new KP regulations, UAE customs officials are authorized to delay or even confiscate those diamonds entering the UAE from another KP member country that does not have the proper certificates.

In 2006, Russian customs officials reportedly apprehended an air passenger from Dubai after he tried to smuggle 2.5 kilos of diamonds into the country. There are also reports that diamonds are increasingly being used as medium to provide countervaluation in hawala transfers, particularly between Dubai and Mumbai. Also in December 2006 a UN report noted that UAE authorities released a suspicious shipment of diamonds after a scientific examination proved that the origin of the

diamonds had been falsified. The UN group felt there were reasonable grounds to pursue a judicial investigation rather than releasing the diamonds to the importer.

The Securities and Commodities Authority (SCA) supervises the country's two stock markets. In February 2004, the SCA issued anti-money laundering guidelines to all brokers that included identity verification instructions for new customer accounts, a reporting requirement for cash transactions above $10,900, and a minimum five-year record keeping requirement for all customer account information. The SCA also instructed brokers to file suspicious transaction reports with the SCA for initial analysis before they are forwarded to the AMLSCU for further action.

Dubai's real estate market continued to show significant growth during 2006, making this sector another area that is susceptible to money laundering abuse. In 2002, Dubai began to allow three real estate companies to sell "freehold" properties to noncitizens. Since then, several other emirates have followed suit. For instance, Abu Dhabi has passed a property law, which provides for a type of lease-hold ownership for noncitizens. In addition, citizens of GCC countries have the right to purchase and trade land within designated investment areas, while other expatriates are permitted to invest in real estate properties for a 99-year leasehold basis. Due to the intense interest in and reported cash purchases of such properties, the potential for money laundering has become of increased concern to the UAE Government. As a result, developers have stopped accepting cash purchases for these properties.

Since the September 11, 2001 terrorist attacks, the UAE Government has been more sensitive to regulating charitable organizations and accounting for funds transfers abroad. In 2002, the UAEG mandated that all licensed charities interested in transferring funds overseas must do so via one of three umbrella organizations: the Red Crescent Authority, the Zayed Charitable Foundation, or the Muhammad Bin Rashid Charitable Trust. These three quasi-governmental bodies are in a position to ensure that overseas financial transfers go to legitimate parties. As an additional step, the UAEG has contacted the governments in numerous aid receiving countries to compile a list of recognized acceptable recipients for UAE charitable assistance.

Charities in Abu Dhabi and the Northern Emirates are regulated by the UAE Ministry of Social Affairs, which is responsible for licensing and monitoring registered charities in these emirates. The Ministry also requires these charities to keep records of all donations and beneficiaries, and to submit financial reports annually. Charities in Dubai are licensed and monitored by the Dubai Department of Islamic Affairs and Charitable Activities. Some charities however, particularly those located in the Northern Emirates, are only registered with their local emirate authority and not the federal Ministry. In July 2006, Regulation 24/2000 was amended, requiring charities from all emirates to obtain a certificate from the Minister of Social Affairs before being permitted to open or maintain bank accounts in the UAE. This amendment effectively required that all charities must be registered federally and no longer at just the emirate level. In November 2006, the UAE hosted a United Kingdom/Gulf Cooperation Council conference on charities, and made a proposal to hold biannual meetings going forward with the UK and GCC on charities oversight.

The UAE has both free trade zones (FTZs) and financial free zones (FFZs). The number of free trade zones (FTZs) is growing, with 26 operating in Dubai and six more in the other emirates. Every emirate except Abu Dhabi has at least one functioning FTZ. The free trade zones are monitored by the local emirate rather than federal authorities.

There are over 5,000 multinational companies located in the FTZs, and thousands more individual trading companies. The FTZs permit 100 percent foreign ownership, no import duties, full repatriation of capital and profits, no taxation, and easily obtainable licenses. Companies located in the free trade zones are considered offshore or foreign entities for legal purposes. However, UAE law prohibits the establishments of shell companies and trusts, and does not permit nonresidents to open bank accounts in the UAE. The larger FTZs in Dubai (such as Jebel Ali free zone) are well-regulated. Although some

trade-based money laundering undoubtedly occurs in the large FTZs, a higher potential for financial crime and exists in some of the smaller FTZs located in the northern emirates.

In March 2004, the UAEG passed Federal Law No. 8, regarding the Financial Free Zones (FFZs) (Law No. 8/2004). Although the new law exempts FFZs and their activities from UAE federal, civil, and commercial laws, FFZs and their operations are still subject to federal criminal laws including the Anti-Money Laundering Law (Law No. 4/2002) and the Anti-Terror Law (Law No. 1/2004). As a result of Law 8/2004 and a subsequent federal decree, the UAE's first financial free zone (FFZ), known as the Dubai International Financial Center (DIFC), was established in September 2004. By September 2005, the DIFC had opened its securities market or the Dubai International Financial Exchange (DIFX).

Law No. 8/2004 limits the issuance of licenses for banking activities in the FFZs to branches of companies, joint companies, and wholly owned subsidiaries provided that they "enjoy a strong financial position and systems and controls, and are managed by persons with expertise and knowledge of such activity." The law prohibits companies licensed in the FFZ from dealing in UAE currency (i.e., dirham), or taking "deposits from the state's markets." Further, the law stipulates that the licensing standards of companies "shall not be less than those applicable in the state." The law empowers the Emirates Stocks and Commodities Authority to approve the listing of any company listed on any UAE stock market in the financial free zone, as well as the licensing of any UAE stock broker. Insurance activities conducted in the FFZ are limited by law to reinsurance contracts only. The law further gives competent authorities in the Federal Government the power to inspect financial free zones and submit their findings to the UAE cabinet.

DIFC regulations provide for an independent regulatory body, namely the Dubai Financial Services Authority (DFSA), to report its findings directly to the office of the Dubai Crown Prince and an independent Commercial Court. According to DFSA regulators, the DFSA due diligence process is a risk-based assessment that examines a firm's competence, financial soundness, and integrity. Prior to the inauguration of the DIFC in 2004, several observers called into question the independence of the DFSA as a result of the high profile firings of the chief regulator and the head of the regulatory council (i.e., the supervisory authority). Subsequent to the firings, Dubai passed laws that gave the DFSA more regulatory independence from the DIFC, although these laws have not yet been tested. The DFSA, who modeled its regulatory regime after the United Kingdom, is the sole authority responsible for issuing licenses to those firms providing financial services in the DIFC.

The DFSA has licensed 94 financial institutions to operate within the DIFC. The DFSA prohibits offshore casinos or internet gaming sites in the UAE, and requires firms to send suspicious transaction reports to the AMLSCU (along with a copy to the DFSA). To date, there have been 9 suspicious transaction reports issued from firms operating in the DIFC (8 in 2006). Although firms operating in the DIFC are subject to Law No. 4/2002, the DFSA has issued its own anti-money laundering regulations and supervisory regime, which has caused some ambiguity about the Central Bank's and the AMLSCU's respective authorities within the DIFC. Ongoing discussions continue between the DFSA and the UAE Central Bank to create a formal bilateral arrangement. The DFSA has undertaken a campaign to reach out to other international regulatory authorities to facilitate information sharing. As of December 2006, the DFSA has MOUs with 16 other regulatory bodies, including the UK's Financial Services Authority (FSA), the Emirates Securities and Commodities Authority, and the U.S. Commodity Futures Trading Commission (CFTC).

The UAE is a party to the 1988 UN Drug Convention and to all twelve UN conventions and protocols relating to the prevention and suppression of international terrorism. It has signed and ratified the UN Convention against Corruption. The UAE has signed, but has not yet ratified the UN Convention against Transnational Organized Crime. The UAE supported the creation of the Middle East and North

Africa Financial Action Task Force (MENAFATF), and, in November 2004, was one of its original charter signatories.

The Government of the UAE has demonstrated progress in constructing a far-reaching anti-money laundering and counterterrorist finance program. Information sharing between the AMLSCU and foreign FIUs has substantially improved. However, several areas requiring further action by the UAEG remain. The most troublesome is the lack of prosecutions and convictions. Law enforcement and customs officials also need to proactively recognize money laundering activity and develop cases based on investigations, rather than wait for case referrals from the AMLSCU that are based on SARs. Additionally, law enforcement and customs officials should conduct more thorough inquiries into large and undeclared cash imports into the country, as well as require—and enforce—outbound declarations of cash and gold. All forms of trade-based money laundering must be given greater scrutiny by UAE customs and law enforcement officials, including customs fraud, the trade in gold and other commodities related to hawala transactions, and the misuse of trade to launder narcotics proceeds. The UAE should increase the resources it devotes to investigation of AML/CFT both at the federal level at the AMLSCU and at the emirate level law enforcement. The UAE's initiatives in the registration of hawaladars should be coupled with investigations. The cooperation between the Central Bank and the DFSA needs improvement, and lines of authority need to be clarified. The UAE should conduct more follow-up with financial institutions and the MSA regarding the recent tightening of regulations on charities to ensure their registration at the federal level. The UAE should also continue its regional efforts to promote sound charitable oversight, and engage in a public campaign to ensure all local charities are aware of registration requirements. The UAE should ratify the UN Convention against Transnational Organized Crime.

United Kingdom

The United Kingdom (UK) plays a leading role in European and world finance and remains attractive to money launderers because of the size, sophistication, and reputation of its financial markets. Although narcotics are still a major source of illegal proceeds for money laundering, the proceeds of other offenses, such as financial fraud and the smuggling of people and goods, have become increasingly important. The past few years have witnessed the movement of cash placement away from High Street banks and mainstream financial institutions. The use of bureaux de change, cash smugglers (into and out of the UK), and gatekeepers (including solicitors and accountants), the purchase of high-value assets as disguises for illegally obtained money, and credit/debit card fraud has been on the increase since 2002.

The UK has implemented many of the provisions of the European Union's (EU) two Directives on the prevention of the use of the financial system for the purpose of money laundering, and the Financial Action Task Force (FATF) Forty Plus Nine Recommendations. Narcotics-related money laundering has been a criminal offense in the UK since 1986. The laundering of proceeds from other serious crimes has been criminalized by subsequent legislation. Banks and nonbank financial institutions in the UK must report suspicious transactions.

In 2001, money laundering regulations were extended to money service bureaus (e.g., bureaux de change, money transmission companies), and in September 2006, the Government published a review into the regulation and performance of money service businesses in preventing money laundering and terrorist financing. Since 2004, more business sectors are subject to formal suspicious activity reporting (SAR) requirements, including attorneys, solicitors, accountants, real estate agents, and dealers in high-value goods such as cars and jewelry. Sectors of the betting and gaming industry that are not currently regulated are being encouraged to establish their own codes of practice, including a requirement to disclose suspicious transactions.

The Proceeds of Crime Act 2002 (POCA), enacted in February 2003, creates a new criminal offense of failing to disclose suspicious transactions in respect to all crimes, not just "serious," narcotics- or terrorism-related crimes, as was the case previously. This is applicable to all regulated sectors. Along with the Act came an expansion of investigative powers relative to large movements of cash in the UK. Sections 327 to 340 of the Act address possession, acquisition, transfer, removal, use, conversion, concealment or disguise of criminal or terrorist property, inclusive of but not limited to money. The POCA also criminalizes tipping off. In 2003, the Financial Secretary to the treasury laid down the "Money Laundering Regulations 2003," along with amending orders for the POCA and the Terrorism Act. The Regulations impose requirements on various entities, including attorneys, and introduce a client identification requirement, requirements on record keeping, internal reporting procedures and training. These regulations came into force on March 1, 2004. In June 2006, a solicitor was sentenced to fifteen months' imprisonment when he was found to have "closed his eyes to the obvious" and been willfully blind to the money laundering offenses committed by his client.

The UK's banking sector provides accounts to residents and nonresidents, who can open accounts through private banking activities and various intermediaries that often advertise on the Internet and also offer various offshore services. Private banking constitutes a significant portion of the British banking industry. Both resident and nonresident accounts are subject to the same reporting and record keeping requirements. Individuals typically open nonresident accounts for tax advantages or for investment purposes.

Bank supervision falls under the Financial Services Authority (FSA). The FSA's primary responsibilities relate to the safety and soundness of the institutions under its jurisdiction. The FSA also plays an important role in the fight against money laundering through its continued involvement in the authorization of banks, and investigations of money laundering activities involving banks. The FSA regulates some 29,000 firms, which include European Economic Area (EEA) firms passporting into the UK (firms doing business on a cross-border basis), ranging from global investment banks to very small businesses, and around 165,000 individuals. From October of 2003, the FSA increased its regulatory role to include mortgage and general insurance agencies, totaling over 30,000 institutions. The FSA administers a civil-fines regime and has prosecutorial powers. The FSA has the power to make regulatory rules with respect to money laundering, and to enforce those rules with a range of disciplinary measures (including fines) if the institutions fail to comply. In October 2006, the financial services sector adopted National Occupational Standards of Competence in the fields of compliance and in anti-money laundering.

Effective July 1, 2005, the Serious Organized Crime and Police Act of 2005 (SOCAP) made changes to the money laundering provisions in the POCA. One of these changes was the creation of the Serious Organized Crime Agency (SOCA), which became the UK's financial intelligence unit (FIU). On April 1, 2006, SOCA took over all FIU functions from the National Criminal Intelligence Service (NCIS). In light of that change SARs are now filed with SOCA. In the context of the SARs regime, SOCAP gives SOCA all the FIU powers and functions that were inherited from NCIS. SOCA has three functions: the prevention and detection of serious organized crime; the mitigation of the consequences of such crime; and the function of receiving, storing, analyzing and disseminating information. Under the law, SOCA's functions are not restricted to serious or organized crime but potentially bear on all crimes, and those functions are to include assistance to others in the discharge of their enforcement responsibilities. In 2005, SOCA's precursor agency NCIS received just under 200,000 SARs and has seen a steady increase each year since 2001. The new law also affected reporting requirements: requirements were relaxed slightly to allow banks to proceed with low value transactions (not exceeding 250 pounds) involving suspected criminal property without requiring specific consent to operate the account. However, the reporting of every such transaction is still required, and other obligated entities were not granted these relaxed standards. Another change that the SOCAP made was that acts would no longer be considered to be money laundering if the act and the property gained took

place in a foreign jurisdiction where the conduct in question was not contrary to the law of the foreign jurisdiction.

The Third Money Laundering Directive was adopted under the UK's presidency of the EU in October 2005. It represents Europe's commitment to fighting the international problems of money laundering and terrorist financing by implementing the global standards produced by the Financial Action Task Force in 2003. The UK Government must implement the Directive into UK law by December 2007. In July 2006, Her Majesty's Treasury released a consultative document discussing how the government seeks to implement the directive. It identifies the areas in which changes need to be made to the Money Laundering Regulations and areas where the Government has flexibility over implementation, and discusses the options available.

The Proceeds of Crime Act 2002 has enhanced the efficiency of the forfeiture process and increased the recovered amount of illegally obtained assets. The Act consolidates existing laws on forfeiture and money laundering into a single piece of legislation, and, perhaps most importantly, creates a civil asset forfeiture system for the proceeds of unlawful conduct. It also creates the Assets Recovery Agency (ARA), to enhance financial investigators' power to request information from any bank about whether it holds an account for a particular person. The Act provides for confiscation orders and for restraint orders to prohibit dealing with property. It also allows for the recovery of property that is, or represents, property obtained through unlawful conduct, or that is intended to be used in unlawful conduct. Furthermore, the Act shifts the burden of proof to the holder of the assets to prove that the assets were acquired through lawful means. In the absence of such proof, assets may be forfeited, even without a criminal conviction. The Act gives standing to overseas requests and orders concerning property believed to be the proceeds of criminal conduct. The Act also provides the ARA with a national standard for training investigators, and gives greater powers of seizure at a lower standard of proof. In light of this, Her Majesty's Revenue and Customs (HMRC) has increased its national priorities to include investigating the movement of cash through money exchange houses and identifying unlicensed money remitters. The total value of assets recovered by all agencies under the Act (and earlier legislation) in England, Wales, and Northern Ireland was approximately $96.6 million in 2004 and approximately $149.6 million in 2005. The Assets Recovery Unit had announced additional seizures worth approximately $30 million in 2006 with an additional $200 million under restraint pending the outcome of court cases.

The Terrorism (United Nations Measures) Order 2001 makes it an offense for any individual to make any funds for financial or related services available, directly or indirectly, to or for the benefit of a person who commits, attempts to commit, facilitates, or participates in the commission of acts of terrorism. The Order also makes it an offense for a bank or building society to fail to disclose to the Treasury a suspicion that a customer or entity with whom the institution has had dealings since October 10, 2001, is attempting to participate in acts of terrorism. The Anti-Terrorism, Crime, and Security Act 2001 provides for the freezing of assets. In March 2006, the Terrorism Act received Royal Assent. This Act aims to impede the encouragement of others to commit terrorist acts, and amends existing legislation. Changes include: the introduction of warrants to enable police to search any property owned or controlled by a terrorist suspect, the extension of terrorism stop and search powers to cover bays and estuaries, with improved search powers at ports, the extension of police powers to detain suspects after arrest for 28 days (although intervals exceeding two days must be approved by a judicial authority), and the increased flexibility of the proscription regime, including the power to proscribe groups that glorify terrorism. As of October 2006, the UK had frozen a total of 188 accounts and approximately $966,000 in suspected terrorist funds.

As a direct result of the events of September 11, 2001, the FID established a separate National Terrorist Financing Investigative Unit (NTFIU), to maximize the effect of reports from the regulated sector. The NTFIU chairs a law enforcement group to provide outreach to the financial industry concerning requirements and typologies. The NTFIU is now under the remit of SOCA. The

operational unit that responds to the work and intelligence development of the NTFIU has seen a threefold increase in staffing levels directly due to the increase in the workload. The Metropolitan Police responded to the growing emphasis on terrorist financing by expanding the focus and strength of its specialist financial unit dedicated to this area of investigations.

Charitable organizations and foundations are subject to supervision by the UK Charities Commission. Such entities must be licensed and are subject to reporting and record keeping requirements. The Commission has investigative and administrative sanctioning authority, up to and including the authority to remove management, appoint trustees and place organizations into receivership. The Government intends to revise its reporting requirements in 2007 to develop a risk-based approach to monitoring with a new serious incident reporting function for charities.

The UK cooperates with foreign law enforcement agencies investigating narcotics-related financial crimes. The UK is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. In February 2006, the UK ratified both the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. The UK is a member of the FATF. SOCA is an active member of the Egmont Group and has information sharing arrangements in place with the FIUs of the United States, Belgium, France, and Australia. The Mutual Legal Assistance Treaty (MLAT) between the UK and the United States has been in force since 1996 (the United States and UK signed a reciprocal asset sharing agreement in March 2003). The UK also has an MLAT with the Bahamas. Additionally, there is a memorandum of understanding in force between the U.S. Immigration and Customs Enforcement and HM Revenue and Customs.

The United Kingdom should develop legislation and implementing regulations to ensure that the gaming and betting industries are completely covered in the same manner as the financial and designated nonfinancial businesses and professions. This should include a legal requirement to disclose suspicious transactions rather than relying on the industries' own codes of practice. In addition, authorities should track and examine the effects of the SOCAP change regarding acts and assets in or from foreign jurisdictions, and revisit this legislation to determine whether it has been effective, or whether it has enabled exploitation.

Uruguay

In the past, Uruguay's strict bank secrecy laws, liberal currency exchange, capital mobility regulations and overall economic stability made it a regional financial center vulnerable to money laundering, though the extent and the nature of suspicious financial transactions have been unclear. In 2002, banking scandals and mismanagement, along with massive withdrawals of Argentine deposits, led to a near collapse of the Uruguayan banking system, significantly weakening Uruguay's role as a regional financial center. This crisis may have diminished the attractiveness of Uruguayan financial institutions for money launderers in the medium term. However, Uruguay's status as an offshore financial center and partially dollarized economy may increase the risk of money laundering and terrorist financing activity.

Fiduciary (offshore) companies called "SAFIs" are thought to be a convenient conduit for illegal money transactions. As of January 1, 2006, all SAFIs are required to provide the names of their directors to the Finance Ministry. In addition, the GOU has decided to completely eliminate SAFIs as part of a comprehensive tax reform law that will be presented to the legislature this year. The draft legislation will also implement a personal income tax for the first time in Uruguay.

Offshore banks are subject to the same laws and regulations as local banks, with the Government of Uruguay (GOU) requiring them to be licensed through a formal process that includes a background investigation. There are six offshore banks and 21 representative offices of foreign banks. Offshore trusts are not allowed. Bearer shares may not be used in banks and institutions under the authority of

the Central Bank, and any share transactions must be authorized by the Central Bank. There are eight free trade zones in Uruguay, all but two being little more than warehouses for regional distribution. The other two house software development firms, back-office operations, call centers, and some light manufacturing and assembly. Some of the warehouse-style free trade zones have been used as transit points for containers of counterfeit goods bound for Brazil and Paraguay. Recent U.S. law enforcement investigations have also revealed suspected funds from the Triborder Area between Argentina, Brazil and Paraguay moving through money remittance companies located in Uruguay.

Over the past five years, the GOU has instituted several legislative and regulatory reforms in its anti-money laundering regime. The May 2001 Law 17,343 extends the predicate offenses beyond narcotics trafficking and corruption to include terrorism; smuggling (value over $20,000); illegal trafficking in weapons, explosives and ammunition; trafficking in human organs, tissues and medications; trafficking in human beings; extortion; kidnapping; bribery; trafficking in nuclear and toxic substances; and illegal trafficking in animals or antiques. Money laundering is considered a crime separate from underlying offenses.

The courts have the power to seize and confiscate property, products or financial instruments linked to money laundering activities. The Central Bank also has the authority to freeze assets for 72 hours, pending a judicial decision. The banking community generally cooperates well with enforcement efforts. There is no specific system for sharing assets with foreign counterparts, but in theory it would be allowed under the provisions of treaties and agreements signed by Uruguay. There is, however, close cooperation with the United States in the sharing of intelligence related to investigations and proceedings. A recent case involving the largest cocaine seizure in Uruguay's history was aided by an unprecedented level of cooperation with U.S. and other foreign law enforcement authorities.

In September 2004, the Uruguayan Congress approved Law 17,835, which significantly strengthens the GOU's money laundering regime. It also includes specific provisions related to the financing of terrorism and to the freezing of assets linked to terrorist organizations, as well as to undercover operations and controlled deliveries. The first arrest and prosecution for money laundering under the new legislation occurred in October 2005, and the case is still pending. A more recent high profile case, involving money laundering linked to Uruguay's largest cocaine seizure, is at the initial stage. Indications are that this case has invigorated the GOU's efforts to fight money laundering and to push for increased reporting of suspicious activities.

Law 17,835 of 2004 expands the realm of entities required to file suspicious activities reports (SARs) and makes reporting of such activities a legal obligation. It specifically confers to Uruguay's financial intelligence unit (FIU), the Financial Information and Analysis Unit (UIAF) of the Central Bank, the role of receiving and analyzing SARs, and disseminating those reports that warrant further investigation to judicial authorities, such as the National Police or the Ministry of the Public Prosecutor. The UIAF also has the authority to request additional related information from obligated reporting entities. Central Bank Circular 1722 of 2000, which created the UIAF, provides the authority to respond to requests for international cooperation. The UIAF is also empowered to issue instructions to the institutions supervised by the Central Bank for them to bar, for a period of up to 72 hours, all transactions involving individuals or legal entities under reasonable suspicion of being linked to the crimes of money laundering and related offenses. The decision must be communicated immediately to the competent criminal court, which will determine, if needed, the freezing of the assets of the parties involved.

In November 2004, Resolution 2002-2072 of the Central Bank Board of Directors raised the UIAF to the level of a directorate reporting directly to the Board. Central Bank regulations require all banks, currency exchange houses, stockbrokers and insurance companies to implement anti-money laundering policies. These policies include thoroughly identifying customers, recording transactions over $10,000 in internal databases, and reporting suspicious transactions to the UIAF. Law 17,835

makes the implementation of these policies a legal obligation extended to all financial intermediaries, including casinos, dealers in art and precious stones and metals, and real estate and fiduciary companies. The law also extends legal protection to reporting institutions for filing SARs. Additionally, Law 17,835 extends the reporting requirement to all persons entering or exiting Uruguay with over $10,000 in cash or in monetary instruments. Regulations for Law 17,835 have been issued by the Central Bank for all entities it supervises, and are being issued by the Ministry of Economy and Finance for all other reporting entities, such as casinos, real estate brokers and art dealers. Although now deemed obligated entities by law, many sectors—including insurance companies, securities firms, money remitters, casinos and most designated nonfinancial businesses—do not yet report suspicious transactions to the UIAF.

The UIAF received 62 SARs in the first 9 months of 2006, almost double the amount received over the same period in 2005. Over the first 9 months of 2006, the UIAF also received 9 action requests from the courts and 15 information requests from foreign FIUs. While the level of staffing at the UIAF is not considered to be adequate, the Central Bank has hired additional staff and established a timeline to reach full staffing. The recent high profile narcotics money laundering case is expected to provide a boost to the Central Bank's efforts.

Three government bodies are responsible for coordinating GOU efforts to combat money laundering: the UIAF, the National Drug Council and the Center for Training on Money Laundering (CECPLA). The President's Deputy Chief of Staff heads the National Drug Council, which is the senior authority for anti-money laundering policy. The Director of CECPLA serves as coordinator for all government entities involved in anti-money laundering efforts, and sets general policy guidelines. The Director defines and implements GOU policies, in coordination with the Finance Ministry and the UIAF. The Ministry of Economy and Finance, the Ministry of the Interior (via the police force), and the Ministry of Defense (via the Naval Prefecture) also participate in anti-money laundering efforts. The financial private sector, most of which is foreign-owned, has developed self-regulatory measures against money laundering such as the Codes of Conduct approved by the Association of Banks and the Chamber of Financial Entities (1997), the Association of Exchange Houses (2001), and the Securities Market (2002).

Despite the power of the courts to confiscate property linked to money laundering, real estate ownership is not publicly registered in the name of the titleholder, complicating efforts to track money laundering in this sector, especially in the partially foreign-owned tourist industry. The UIAF and other government agencies must obtain a judicial order to have access to the name of titleholders. The GOU is in the process of implementing a national computerized registry that will facilitate the UIAF's access to titleholders' names.

Uruguay is a founding member of the Financial Action Task Force for South America (GAFISUD), created in December 2000 and based in Buenos Aires. Since early 2005, the ex-director of the Center for Training on Money Laundering Issues (CECPLA) has served as the GAFISUD Executive Secretary. In 2005, the International Monetary Fund (IMF), in conjunction with GAFISUD, concluded the second mutual evaluation of Uruguay's anti-money laundering and counterterrorist financing regime. Their report was presented at the GAFISUD plenary meeting in July 2006. The evaluation recognized Uruguay's advances with its new legislation but pointed out that some regulations still needed to be drafted in order to fully implement the legislative reforms. The evaluation team did not consider the UIAF to be fully operational due to understaffing and limited resources.

The GOU has taken steps to bring Uruguay into compliance with the Financial Action Task Force (FATF) Special Recommendations on Terrorist Financing. Some of these recommendations, such as the criminalization of terrorism financing and provisions for the freezing of terrorist assets, were partially met by Law 17,835. Law 17,835 establishes a prison term of three to 18 years for terrorist financing, requires financial institutions inform the UIAF of funds that may be connected to persons

on the United Nations 1267 Sanctions Committee list and individual country lists, and allows for the freezing of terrorist funds. However, as noted by the IMF and GAFISUD mutual evaluation team, terrorist financing is a crime only to the extent that funds are collected or solicited for terrorist acts. The provision of funds to terrorists or terrorist groups, for purposes other than planned or committed acts of terrorism, is not specifically criminalized. Although terrorism is considered a predicate offense for money laundering, terrorism is not criminalized under Uruguayan law; Law 17,835, however, does establish criteria for determining the "terrorist nature" of an offense. Nonprofit organizations are not assessed for terrorist financing risk, and oversight of these institutions was deemed by the IMF/GAFISUD evaluation team to be insufficient.

The GOU states that safeguarding the financial sector from money laundering is a priority, and Uruguay remains active in international anti-money laundering efforts. Uruguay is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime. It has signed, but not yet ratified, the UN Convention against Corruption and the Inter-American Convention against Terrorism. The GOU is a member of GAFISUD and the OAS Inter-American Drug Abuse Control Commission (CICAD) Experts Group to Control Money Laundering. The United States and Uruguay are parties to extradition and mutual legal assistance treaties that entered into force in 1984 and 1994, respectively.

In 2006, the Government of Uruguay continued to implement the reforms it began in 2004 and 2005 to strengthen its anti-money laundering and counterterrorist financing regime. The passage of legislation criminalizing terrorist financing, albeit limited only to the financing of terrorist acts, places Uruguay ahead of many other nations in the region. Nevertheless, the GOU should amend its legislation to make the funding of terrorists or terrorist organizations a crime. Uruguay is one of only two countries in South America that is not a member of the Egmont Group of financial intelligence units. Membership in the Egmont Group would provide the GOU with greater access to financial information that is essential to its efforts to combat money laundering and terrorist financing. The UIAF's membership in the Egmont Group, as well as the GOU's continued implementation, enhancement and enforcement of its anti-money laundering and counterterrorist financing programs, should continue to be priorities for the GOU.

Uzbekistan

Uzbekistan is not considered an important regional financial center and does not have a well developed financial system. Legitimate business owners, ordinary citizens, and foreign residents generally attempt to avoid using the Uzbek banking system for transactions, except when absolutely required, because of the nature of the Government of Uzbekistan's (GOU) financial control system, the fear of GOU seizure of one's assets, and the lack of trust in the banking system as a whole. As a result, Uzbek citizens have functioning bank accounts only if they are required to do so by law. Citizens only deposit funds they are required to deposit and often resort to subterfuge to avoid depositing currency. The Central Bank of Uzbekistan (CB) asserts that deposits from individuals have been increasing over the past four years.

Proceeds from narcotics and black market smuggling are primary sources of money laundering. Narcotics proceeds are controlled by local and regional drug-trafficking organizations and organized crime. Foreign and domestic proceeds from criminal activity in Uzbekistan are held either in cash, high-value transferable assets, such as gold, property, or automobiles, or in foreign bank accounts.

There is a significant black market for smuggled goods in Uzbekistan. Since the GOU imposed a very restrictive trade and import regime in the summer of 2002, smuggling of consumer goods, already a considerable problem, increased dramatically. Many Uzbek citizens continue to make a living by illegally shuttle-trading goods from neighboring countries, Iran, the Middle East, India, Korea, Europe, and the U.S. The black market for smuggled goods does not appear to be significantly funded

by narcotics proceeds. It is likely, however, that drug dealers use the robust black market to clean their drug-related money.

Reportedly, the unofficial, unmonitored cash-based market creates an opportunity for small-scale terrorist or drug-related laundering of funds destined for internal operations. For the most part, the funds generated by smuggling and corruption are not directly laundered through the banking system, but through seemingly legitimate businesses such as restaurants and high-end retail stores. There appears to be virtually no money laundering through formal financial institutions in Uzbekistan because of the extremely high degree of supervision and control over all bank accounts in the country exercised by the CB, Ministry of Finance, General Prosecutor's Office (GPO), and state-owned and controlled banks. Although Uzbek financial institutions are not known to engage in illegal transactions in U.S. currency, illegal unofficial exchange houses, where the majority of cash-only money laundering takes place, deal in Uzbek soum and U.S. dollars. Moreover, drug dealers and others can transport their criminal proceeds in currency across Uzbekistan's porous borders for deposit in the banking systems of other countries, such as Kazakhstan, Russia or the United Arab Emirates.

Laundering the proceeds of drug-trafficking and other criminal activities is a criminal offense. Article 41 of the Law on Narcotic Drugs and Psychotropic Substances (1999) provides that any institution may be closed for performing a financial transaction for the purpose of legalizing (laundering) proceeds derived from illicit narcotics trafficking. Penalties for money laundering are from ten to fifteen years' imprisonment, under Article 243 of the Criminal Code. This article defines the act of money laundering to include as punishable acts the transfer, conversion, exchange, or concealment of origin, true nature, source, location, disposition, movement and rights with respect to the assets derived from criminal activity. Although the law has been in effect for more than five years, the GOU has been unable to provide sufficient information to fully assess the implementation and use of this legislation. The GOU has not adopted "banker negligence" laws that hold individual bankers responsible if their institutions launder money.

The CB, GPO, and the National Security Service (NSS) closely monitor all banking transactions to ensure that money laundering does not occur in the banking system. Banks are required to know, record, and report the identity of customers engaging in significant transactions, including the recording of large currency transactions at thresholds appropriate to Uzbekistan's economic situation. All transactions involving sums greater than $1000 in salary expenses for legal entities and $500 in salaries for individuals must be tracked and reported to the authorities. The CB unofficially "requires" commercial banks to report on private transfers to foreign banks exceeding $10,000. Depending on the type and amount of the transaction, banks are required to maintain records for time deposits for a minimum of five years. The law contains a safe harbor provision, protecting reporting individuals with respect to their cooperation with law enforcement entities.

In 2004, Uzbekistan's Parliament passed the Law on the Fight Against Legitimization of Proceeds of Crime and Combating Terrorism Financing, which went into effect on January 1, 2006. The law requires certain entities to report cash transactions above $40,000 (approximately), as well as suspicious transactions. Banks, credit unions and other lending institutions are covered entities. The law also covers some nonbanking financial institutions, such as investment funds, depositaries and other types of investment institutions; exchange houses; insurers; organizations which render leasing and other financial services; postal organizations; pawnshops; gaming houses; lotteries; and notary offices. It does not include intermediaries such as lawyers, accountants, or broker/dealers. Although casinos are illegal, GOU enforcement is generally lax, and several exist openly in Tashkent.

The Law on Banks and Bank Activity (1996), article 38, stipulates conditions under which banking information can be released to law enforcement, investigative and tax authorities, prosecutor's office and courts. Different conditions for disclosure apply to different types of clients—individuals and institutions. In September 2003, Uzbekistan enacted a bank secrecy law that prevents the disclosure of

client and ownership information for domestic and offshore financial services companies to bank supervisors and law enforcement authorities. In all cases, private bank information can be disclosed to prosecution and investigation authorities, provided there is a criminal investigation underway. The information can be provided to the courts on the basis of a written request in relation to cases currently under consideration. Protected banking information also can be disclosed to tax authorities in cases involving the taxation of a bank's client. Additionally, under a new 2006 Presidential decree and subsequent Cabinet of Ministers' resolution on the disclosure of information related to money laundering, it is mandatory for organizations involved in monetary and other transactions to report such transactions to a new Financial Intelligence Unit within the GPO (discussed below).

Existing controls on transportation of currency across borders would, in theory, facilitate detection of the international transportation of illegal source currency. When entering or exiting the country, foreigners and Uzbek citizens are required to report all currency they are carrying. Residents and nonresidents may bring the equivalent of $10,000 into the country tax-free. Amounts in excess of this limit are assessed a one-percent duty. Nonresidents may take out as much currency as they brought in. However, residents are limited to the equivalent of $2,000. Residents wishing to take out higher amounts must obtain authorization to do so; amounts over $2,000 must be approved by an authorized commercial bank, and amounts over $5,000 must be approved by the CB. International cash transfers to or from an individual person are limited to $5,000 per transaction; there is no monetary limit on international cash transfers made by legal entities, such as corporations. However, direct wire transfers to or from other Central Asian countries are not permitted; a third country must be used.

International business companies are permitted to have offices in Uzbekistan and are subject to the same regulations as domestic businesses, if not stricter. Offshore banks are not present in Uzbekistan and other forms of exempt or shell companies are not officially present.

In April 2006, the President of Uzbekistan signed a decree entitled, "On Actions to Strengthen Combating Financial, Economic and Tax Crimes and Legalization of Criminally Gained Income." This decree expands the mandate of the General Prosecutor's Office for Combating Tax and Hard Currency Crimes to include combating money laundering, and established the Department on Combating Tax, Currency Crimes and Legalizations of Criminal Proceeds under the GPO. This Department, which will serve as Uzbekistan's Financial Intelligence Unit (FIU), will conduct operational, analytical and investigative work in the areas of tax and hard currency crimes, money laundering and terrorism financing. The FIU is charged with monitoring and preventing money laundering and terrorist financing. It will analyze information received from banks and financial institutions, create and keep electronic databases of financial crimes, and, when warranted, pass information to the CB, tax and law enforcement authorities, or other parts of the GPO for investigation and prosecution of criminal activity. Authorities envisage a staff of 22 people in the FIU. The Department of Investigation of Economic Crimes within the Ministry of Internal Affairs (MVD) and a specialized structure within the NSS also are authorized to conduct investigations of money laundering offenses.

In the coming year, the new FIU analysts and investigators, as well as authorities in related ministries and agencies, will require training and capacity building for the FIU. Uzbekistan has entered into agreements with supervisors to facilitate the exchange of supervisory information including on-site examinations of banks and trust companies operating in the country. Since September 2006, the Uzbek financial supervisory authorities, along with law enforcement officers, have been attending World Bank-sponsored workshops to acquaint them with the AML/CFT law. These workshops will continue into May 2007.

In July 2006, the Uzbek Cabinet of Ministers adopted a resolution on the submission of data to the FIU related to money laundering and terrorism financing.

Unofficial information from numerous law enforcement officials indicates that there have been few, if any, prosecutions for money laundering under article 243 of the Criminal Code since its enactment in 2001. MVD officials claim to have opened nine money laundering-related cases in 2005 and six cases in the first six months of 2006. No information was provided on the ultimate disposition of these cases. In March 2006, an opposition activist was convicted for money laundering and other economic crimes, but the defendant was freed in May and the sentence was suspended, reportedly due to human rights questions surrounding the case. Overall, the GOU appears to lack a sufficient number of experienced and knowledgeable agents to investigate money laundering.

Article 155 of Uzbekistan's Criminal Code and the law "On Fighting Terrorism" criminalize terrorist financing. The latter law names the NSS, the MVD, the Committee on the Protection of State Borders, the State Customs Committee, the Ministry of Defense, and the Ministry for Emergency Situations as responsible for implementing the counterterrorist legislation. The law names the NSS as the coordinator for government agencies fighting terrorism. The GOU has the authority to identify, freeze, and seize terrorist assets. Uzbekistan has circulated to its financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee's consolidated list and the names of individuals and entities included on the UN 1267 consolidated list. In addition, the GOU has circulated the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224 to the CB, which has, in turn, forwarded these lists to banks operating in Uzbekistan. According to the CB, no assets have been frozen.

Other than a plan to step up enforcement of currency regulations, the GOU has taken no steps to regulate or deter alternative remittance systems such as hawala, black market exchanges, trade-based money laundering, or the misuse of gold, precious metals and gems, nor are any legislative initiatives addressing alternative remittance under consideration. Although officially there is complete currency convertibility, in reality convertibility requests can be significantly delayed or refused. The GOU took additional steps in the second half of 2005 to further restrict convertibility, leading to a slightly higher black market exchange rate for the soum.

The GOU closely monitors the activities of charitable and nonprofit entities, such as NGOs, that can be used for the financing of terrorism. In February 2004, the Cabinet of Ministers issued Decree 56 to allow the government to vet grants to local NGOs from foreign sources, ostensibly to fight money laundering and terrorist financing. Given the degree of supervision of charities and other nonprofits, and the level of threat Uzbekistan perceives from the Islamic Movement of Uzbekistan (IMU) and other extremist organizations, it is extremely unlikely that the NSS would knowingly allow any funds to be funneled to terrorists through Uzbekistan-based charitable organizations or NGOS.

Uzbekistan has established systems for identifying, tracing, freezing, seizing, and forfeiting proceeds of both narcotics-related and money laundering-related crimes. Current laws include the ability to seize items used in the commission of crimes such as conveyances used to transport narcotics, farm facilities (except land) where illicit crops are grown or which are used to support terrorist activity, legitimate businesses if related to criminal proceeds and bank accounts. The banking community, which is entirely state-controlled and, with few exceptions, state-owned, cooperates with efforts to trace funds and seize bank accounts. Uzbek law does not allow for civil asset forfeiture, but the Criminal Procedure Code provides for "civil" proceedings within the criminal case to decide forfeiture issues. As a practical matter, these proceedings are conducted as part of the criminal case. There appears to be no new legislation or changes to current law under active consideration by the GOU regarding seizure or forfeiture of assets. The obstacles to enacting such laws are largely rooted in the widespread corruption that exists within the country.

In 2000, Uzbekistan set up a fund to direct confiscated assets to law enforcement activities. In accordance with the regulation, the assets derived from the sale of confiscated proceeds and instruments of drug-related offenses were transferred to this fund to support entities of the NSS, the

MVD, the State Customs Committee, and the Border Guard Committee, all of which are directly involved in combating illicit drug trafficking. According to the GOU, a total of 115 million soum (approximately $97,000) was deposited into this fund, roughly $80,000 of which was turned over to Uzbek law enforcement agencies. In 2004, however, the Cabinet of Ministers issued an order to close the Special Fund as of November 1, 2004. Under the new procedures, each agency manages the assets it seizes. There is also a specialized fund within the MVD to reward those officers who directly participate in or contribute to law enforcement efforts leading to the confiscation of property. This fund has generated 20 percent of its assets from the sale of property confiscated from persons who have committed offenses such as the organization of criminal associations, bribery and racketeering. The GOU enthusiastically enforces existing drug-related asset seizure and forfeiture laws. The GOU has not been forthcoming with information regarding the total dollar value of assets seized from crimes. Reportedly, existing legislation does not permit sharing of seized narcotics assets with other governments.

The GOU realizes the importance of international cooperation in the fight against drugs and transnational organized crime and has made efforts to integrate the country in the system of international cooperation. Uzbekistan has entered into bilateral agreements for cooperation or exchange of information on drug related issues with the United States, Germany, Italy, Latvia, Bulgaria, Poland, China, Iran, Pakistan, the CIS, and all the countries in Central Asia. It has multilateral agreements within the framework of the CIS and under the Shanghai Cooperation Organization (SCO). An "Agreement on Narcotics Control and Law Enforcement Assistance" was signed with the United States on August 14, 2001, with two supplemental agreements that came into force in 2004.

Uzbekistan does not have a Mutual Legal Assistance Treaty with the United States. However, Uzbekistan and the United States have reached informal agreement on mechanisms for exchanging adequate records in connection with investigations and proceedings relating to narcotics, terrorism, terrorist financing and other serious crime investigations. In the past, Uzbekistan has cooperated with appropriate USG law enforcement agencies and other governments investigating financial crimes and several important terrorist-related cases. However, cooperation in these areas has become increasingly problematic in an atmosphere of deteriorating U.S.-Uzbekistan bilateral relations.

Uzbekistan joined the Eurasian Group on Combating Money Laundering and the Financing of Terrorism (EAG), a FATF-style regional body, at the group's December 2005 plenary meeting. In April 2006, at the invitation of the Prosecutor General of Uzbekistan, the EAG Chairman visited Tashkent to discuss, in part, Uzbekistan's partnership in the EAG, the progress the country has made in establishing an AML/CFT regime, and technical assistance that will be required. Uzbekistan is scheduled to have an EAG mutual evaluation in 2008.

The GOU is an active party to the relevant agreements concluded under the CIS, CAEC, ECO, SCO, and the "Six Plus Two" Group. In December 2005, Uzbekistan hosted the SCO in Tashkent to discuss issues relating to and the overall prevention of money laundering. Uzbekistan is also 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.

A lack of trained personnel, resources, and modern equipment continues to hinder Uzbekistan's efforts to fight money laundering and terrorist financing. The GOU should ensure that those with supervisory authority and those charged with investigating potential money laundering and terrorism financing have the training and resources necessary to be effective. This includes legal resources as well: the GOU should continue to refine its pertinent legislation to adhere to international standards. Uzbekistan also should expand the cross-border currency reporting rules to cover the transfer of monetary instruments, gold, gems and precious metals. Access to financial institution records should be given to appropriate regulatory and law enforcement agencies so that they can properly conduct compliance

examinations and investigations. Furthermore, while the establishment of a Financial Intelligence Unit is a positive step, its effectiveness will depend on the unit's authority as the sole repository and analytical tool for suspicious transaction reporting. The FIU's ability to effectively cooperate with other GOU law enforcement and regulatory agencies in receiving and disseminating information on suspicious transactions will be critical to the success of an AML/CFT regime. The GOU should ensure that the FIU has the appropriate resources, including the technical requirements for a database, training on analytical, legal and technical elements for the staff, and the authority and bureaucratic tools to meet international standards and accomplish its mandate.

Vanuatu

Vanuatu's offshore sector is vulnerable to money laundering, as Vanuatu has historically maintained strict banking secrecy provisions that have the effect of preventing law enforcement agencies from identifying the beneficial owners of offshore entities registered in the sector. Due to allegations of money laundering, and in response to pressure from the Financial Action Task Force (FATF), a few United States-based banks announced in December 1999 that they would no longer process U.S. dollar transactions to or from Vanuatu. The Government of Vanuatu (GOV) responded to these concerns by introducing reforms designed to strengthen domestic and offshore financial regulation. The GOV passed amendments to four of its main legislations pieces of legislation relative to money laundering and terrorist financing during its last session of Parliament in November 2005. The four pieces of legislation affected are the Mutual Assistance in Criminal Matters Act No. 31 of 2005, the Financial Transaction Reporting Act No. 28 of 2005, the Counter-Terrorism and Transnational Organized Crime Act No. 29 of 2005, and the Proceeds of Crime Act (Amendment) Act No. 30 of 2005.

Vanuatu's financial sector includes four domestic licensed banks (that carry out domestic and offshore business); one credit union; seven international banks; five insurance providers (both life and general); and eight foreign exchange instrument dealers, money remittance dealers and bureaux de change, all of which are regulated by the Reserve Bank of Vanuatu. Since the passage of the International Banking Act of 2002, the Reserve Bank of Vanuatu regulates the offshore banking sector that includes the seven international banks and approximately 4,700 international business companies (IBCs), as well as offshore trusts and captive insurance companies. These institutions were once regulated by the Financial Services Commission. IBCs are now registered with the Vanuatu Financial Services Commission. This change was one of many recommendations of the 2002 International Monetary Fund Module II Assessment Report (IMFR) that found Vanuatu's onshore and offshore sectors to be "noncompliant" with many international standards.

Regulatory agencies in Vanuatu have instituted stricter procedures for issuance of offshore banking licenses under the International Banking Act No. 4 of 2002, and continue to review the status of previously issued licenses. All financial institutions, both domestic and offshore, are required to report suspicious transactions and to maintain records of all transactions for six years, including the identities of the parties involved.

The Financial Transaction Reporting Act (FTRA) of 2000 established Vanuatu's Financial Intelligence Unit (FIU) within the State Law Office. The FIU receives suspicious transaction reports (STRs) filed by banks and distributes them to the Public Prosecutor's Office, the Reserve Bank of Vanuatu, the Vanuatu Police Force, the Vanuatu Financial Services Commission, and law enforcement agencies or supervisory bodies outside Vanuatu. The FIU also issues guidelines to, and provides training programs for, financial institutions regarding record keeping for transactions and reporting obligations. The Act also regulates how such information can be shared with law enforcement agencies investigating financial crimes. Financial institutions within Vanuatu must establish and maintain internal procedures to combat financial crime. Every financial institution is required to keep records of all transactions. Five key pieces of information are required to be kept for every financial

transaction: the nature of the transaction, the amount of the transaction, the currency in which it was denominated, the date the transaction was conducted, and the parties to the transaction.

Although the amendments have been withdrawn from Parliament twice, FTRA amendments were finally passed in November 2005 and enacted in late February 2006. The amendments include mandatory customer identification requirements; broaden the range of covered institutions required to file STRs to include auditors, trust companies, and company service providers; and provide safe harbor for both individuals and institutions required to file STRs. In addition to STR filings, financial institutions will now be required to file currency transaction reports (CTRs), which involves any single transaction in excess of VT 1 million (approximately $9,100) or its equivalent in a foreign currency, and wire transfers into and out of Vanuatu in excess of VT 1 million. The amendments also require financial institutions to maintain internal procedures to implement reporting requirements, appoint compliance officers, establish an audit function to test their anti-money laundering and terrorist financing procedures and systems, as well as provide the FIU a copy of their internal procedures. Failure to do so will result in a fine or imprisonment for an individual, or a fine in the case of a corporate entity. The amendments supersede any inconsistent banking or other secrecy provisions and clarify the FIU's investigative powers.

The amended FTRA defines financial institutions to include casinos licensed under the Casino Control Act No.6 of 1993, lawyers, notaries, accountants and trust and company service providers. The scope of the legislation is so broad that entities such as car dealers and various financial services that currently do not exist in Vanuatu (and are unlikely to in the future) are covered. Applications by foreigners to open casinos are subject to clearance by the Vanuatu Investment Promotion Authority (VIPA) which reviews applications and conducts a form of due diligence on the applicant before issuing a certification of the department of Customs and Revenue to issue an appropriate license. The Department of Customs and Inland Revenue receives applications from local applicants directly.

The Vanuatu Police Department and the FIU are the primary agencies responsible for ensuring money laundering and terrorist financing offences are properly investigated in Vanuatu. The Public Prosecutions Office (PPO) is responsible for the prosecution of money laundering and terrorist financing offences. The Vanuatu Police Department has established a Transnational Crime Unit (TCU), and is responsible for investigations involving money laundering and terrorist financing offences, the identification and seizure of criminal proceeds, as well as conducting investigations in cooperation with foreign jurisdictions.

Supervision of the financial services sector is divided between three main agencies: the Reserve Bank of Vanuatu (RBV), the Vanuatu Financial Services Commission (VFSC) and the Customs and Revenue Branch of the Ministry of Finance. The RBV is responsible for supervising and regulating domestic and off-shore banks. The VFSC supervises insurance providers, credit unions, charities and trust and company service providers, but is unable to issue comprehensive guidelines or to regulate the financial sectors it has responsibility for.

The Serious Offenses (Confiscation of Proceeds) Act 1989 criminalized the laundering of proceeds from all serious crimes and provided for seizure of criminal assets and confiscation after a conviction. The Proceeds of Crime Act (2002) retained the criminalization of the laundering of proceeds from all serious crimes, criminalized the financing of terrorism, and included full asset forfeiture, restraining, monitoring, and production powers regarding assets. A new development to the Proceeds of Crime Act No. 30 of 2005 was an insertion of Section 74A, which now cover the cross-border movement of currency. After the passing of the bill in Parliament in November 2005, all incoming and outgoing passengers to and from Vanuatu will be legally obligated to declare to the Department of Customs cash exceeding one million Vatu in possession (approximately $9,100).

Vanuatu passed the Mutual Assistance in Criminal Matters Act in December 2002 for the purpose of facilitating the provision of international assistance in criminal matters for the taking of evidence,

search and seizure proceedings, forfeiture or confiscation of property, and restraints on dealings in property that may be subject to forfeiture or seizure. The Attorney General possesses the authority to grant requests for assistance, and may require government agencies to assist in the collection of information pursuant to the request. The Extradition Act of 2002 includes money laundering within the scope of extraditable offenses.

The amended International Banking Act has now placed Vanuatu's international and offshore banks under the supervision of the Reserve Bank of Vanuatu. Section 5(5) of the Act states that if existing licensees wish to carry on international banking business after December 31, 2003, the licensee should have submitted an application to the Reserve Bank of Vanuatu under Section 6 of the Act for a license to carry on international banking business. If an unregistered licensee continued to conduct international banking business after December 31, 2003, in violation of Section 4 of the Act, the licensee is subject to a fine or imprisonment. Under Section 19 of the Act, the Reserve Bank can conduct investigations where it suspects that an unlicensed person or entity is carrying on international banking business. Since this time, three international banking businesses have had their licenses revoked.

One of the most significant requirements of the amended legislation is the banning of shell banks. As of January 1, 2004, all offshore banks registered in Vanuatu must have a physical presence in Vanuatu, and management, directors, and employees must be in residence. At the September 2003 plenary session of the Asia/Pacific Group on Money Laundering (APG), Vanuatu noted its intention to draft new legislation regarding trust companies and company service providers, which it is now in the final stages of completing. The new legislation will cover disclosure of information with other regulatory authorities, capital and solvency requirements, and "fit and proper" requirements. In 2005, Vanuatu enacted Insurance Act No. 54, drafted in compliance with standards set by the International Association of Insurance Supervisors.

International Business Companies (IBC) may be registered using bearer shares, shielding the identity and assets of beneficial owners of these entities. Secrecy provisions protect all information regarding IBCs and provide penal sanctions for unauthorized disclosure of information. These secrecy provisions, along with the ease and low cost of incorporation, make IBCs ideal mechanisms for money laundering and other financial crimes. Section 125 of the International Companies Act No. 31 of 1992 (ICA), provides a strict secrecy provision for information disclosure related to shareholders, beneficial ownership, and the management and affairs of IBCs registered in Vanuatu. This provision, in the past, has been used by the industry to decline requests made by the FIU for information. However, section 17(3) of the new amended FTRA clearly states that the new secrecy-overriding provision in the FTRA overrides section 125 of the ICA.

In November 2005, Vanuatu passed the Counter-Terrorism and Transnational Organized Crime Act (CTTOCA) No. 29 of 2005. The CTTOCA was brought into force on 24 February 2006. The aim of the Act is to implement UN Security Council Resolutions and Conventions dealing with terrorism and transnational organized crime, to prevent terrorists from operating in Vanuatu or receiving assistance through financial resources available to support the activities of terrorist organizations, and to criminalize human trafficking and smuggling. Terrorist financing is criminalized under section 6 of the CTTOCA. Section 7 of the CTTOCA makes it an offence to "directly or indirectly, knowingly make available property or financial or other related services to, or for the benefit of, a terrorist group." The penalty upon conviction is a term of imprisonment of not more than 25 years or a fine of not more than VT 125 million ($1 million), or both. Section 8 criminalizes dealing with terrorist property. The penalty upon conviction is a term of imprisonment of not more than 20 years or a fine of not more than VT100 million ($USD 876,500), or both. There were no terrorist financing or terrorism-related prosecutions or investigations in 2006.

In addition to its membership the Asia Pacific Group on Money Laundering, Vanuatu is a member of the Offshore Group of Banking Supervisors, the Commonwealth Secretariat, and the Pacific Island Forum. Its Financial Intelligence Unit became a member of the Egmont Group in June 2002. The GOV acceded to the UN International Convention for the Suppression of the Financing of Terrorism in October 2005, and acceded to both the UN Convention against Transnational Organized Crime and the 1988 UN Drug Convention on January 4, 2006. The FIU has a memorandum of understanding with Australia.

In March 2006, the APG conducted a mutual evaluation of Vanuatu, the results of which were reported at the APG plenary meeting in November 2006. The APG evaluation team found that Vanuatu had improved its anti-money laundering and counterterrorist financing regime since its first evaluation in 2000 by criminalizing terrorist financing, requiring a wider range of entities to report to the FIU and enhancing supervisory oversight of obligated entities. However, some deficiencies remain: the GOV has not taken a risk-based approach to combating money laundering and terrorist financing; a person who commits a predicate offense for money laundering cannot also be charged with money laundering; and current law does not require the names and addresses of directors and shareholders to be provided upon registration of an IBC.

The Government of Vanuatu should immobilize bearer shares and require complete identification of the beneficial ownership of international business companies (IBCs). It should implement all the provisions of its Proceeds of Crime Act and enact all additional legislation that is necessary to bring both its onshore and offshore financial sectors into compliance with international standards.

Venezuela

Venezuela is one of the principal drug-transit countries in the Western Hemisphere, with an estimated 250-300 metric tons of cocaine passing through the nation during 2006. Venezuela's proximity to drug producing countries, weaknesses in its anti-money laundering regime, refusal to cooperate with the United States on counternarcotics activities, and rampant corruption throughout the law enforcement, judicial, banking, and banking regulatory sectors continue to make Venezuela vulnerable to money laundering. The main source of money laundering is believed to be from proceeds generated by cocaine and heroin trafficking organizations. Trade-based money laundering, such as the Black Market Peso Exchange, through which money launderers furnish narcotics-generated dollars in the United States to commercial smugglers, travel agents, investors, and others in exchange for Colombian pesos, remains a prominent method for laundering narcotics proceeds. It is reported that many of these black market traders ship their wares through Venezuela's Margarita Island free trade zone. Reportedly, some money is also laundered through the real estate market in Margarita Island.

Venezuela is not a regional financial center, nor does it have an offshore financial sector. The relatively small but modern banking sector, which consists of 55 banks, primarily serves the domestic market. The majority of these banks, about 90 percent, belong to the Venezuelan Association of Banks. Membership is voluntary and meetings are held monthly.

Money laundering in Venezuela is criminalized under the 2005 Organic Law against Organized Crime, the passage of which broadened the legal mechanisms provided by the 1993 Organic Drug Law. Under the Organic Law against Organized Crime, money laundering is an autonomous offense, punishable by a sentence of eight to twelve years in prison. Those who cannot establish the legitimacy of possessed or transferred funds, or are aware of the illegitimate origins of those funds, can be charged with money laundering, without any connection to drug-trafficking. In addition to establishing money laundering as an autonomous predicate offense, the Organic Law against Organized Crime broadens asset forfeiture and sharing provisions, adds conspiracy as a criminal offense, strengthens due diligence requirements, and provides law enforcement with stronger investigative powers by authorizing the use of modern investigative techniques, such as the use of undercover agents. This law,

coupled with the new Law Against the Trafficking and Consumption of Narcotics and Psychotropic Substances, effectively brings Venezuela's Penal Code in line with the 1988 UN Drug Convention.

In spite of the advances made with the passage of the Organic Law against Organized Crime in 2005, three major gaps remain. First, the financing of terrorism has yet to be specifically criminalized and there is still no independent financial investigative unit. One year after promulgation, there are no money laundering cases being tried under the new law. Many, if not most, judicial and law enforcement officials remain ignorant of the Law against Organized Crime and its specific provisions. Second, widespread corruption within the judicial and law enforcement sectors undermines the effectiveness of the law as a tool to combat the growing problem of money laundering. Finally, there is little evidence that the Government of Venezuela (GOV) has the will to effectively enforce the legislation it has promulgated.

Under the Organic Law against Organized Crime and Resolution 333-97 of the Superintendent of Banks and Other Financial Institutions (SBIF), anti-money laundering controls have been implemented requiring strict customer identification requirements and the reporting of both currency transactions over a designated threshold and suspicious transactions. These controls apply to all banks (commercial, investment, mortgage, and private), insurance and reinsurance companies, savings and loan institutions, financial rental agencies, currency exchange houses, money remitters, money market funds, capitalization companies, frontier foreign currency dealers, casinos, real estate agents, construction companies, car dealerships, hotels and the tourism industry, travel agents, and dealers in precious metals and stones. These entities are required to file suspicious and cash transaction reports with Venezuela's financial intelligence unit (FIU), the Unidad Nacional de Inteligencia Financiera (UNIF. Financial institutions are required to maintain records for a period of five years.

The UNIF was created under the SBIF in July 1997 and began operating in June 1998. Under the original draft of the Organic Law against Organized Crime, the UNIF would have become an autonomous entity with investigative powers, independent of the SBIF, but the relevant clauses were removed just prior to the law's passage. The UNIF has a staff of approximately 55 and has undergone multiple bureaucratic changes, with five different directors presiding over the UNIF since 2004. The SBIF and the UNIF have little credibility within the financial sector, with credible reports indicating that both are used by the government to investigate political opponents.

The UNIF receives suspicious transaction reports (STRs) and reports of currency transactions (CTRs) exceeding approximately $2,100 from institutions regulated by the SBIF, the Office of the Insurance Examiner, the National Securities and Exchange Commission, the Bureau of Registration and Notaries, the Central Bank of Venezuela, and the Bank Deposits and Protection Guarantee Fund, as well as the other entities now included under the Organic Law against Organized Crime. The Venezuelan Association of Currency Exchange Houses (AVCC), which counts all but one of the country's money exchange companies among its membership, voluntarily complies with the same reporting standards as those required of banks. Some institutions regulated by the SBIF, such as tax collection entities and public service payroll agencies, are exempt from the reporting requirement. The SBIF also allows certain customers of financial institutions-those who demonstrate "habitual behavior" in the types and amounts of transactions they conduct-to be excluded from currency transaction reports filed with the UNIF. SBIF Circular 3759 of 2003 requires financial institutions that fall under the supervision of the SBIF to report suspicious activities related to terrorist financing; however, terrorist financing is not a crime in Venezuela.

In addition to STRs and CTRs, the UNIF also receives reports on the domestic transfer of foreign currency exceeding $10,000, the sale and purchase of foreign currency exceeding $10,000, and summaries of cash transactions that exceed approximately $2,100. The UNIF does not, however, receive reports on the transportation of currency or monetary instruments into or out of Venezuela. A system has been developed for electronic receipt of CTRs, but STRs must be filed in paper format.

Obligated entities are forbidden to reveal reports filed with the UNIF or suspend accounts during an investigation without official approval, and are also subject to sanctions for failure to file reports with the UNIF.

The UNIF analyzes STRs and other reports, and refers those deemed appropriate for further investigation to the Public Ministry (the Office of the Attorney General). According to the UNIF, it forwards approximately 30 percent of the STRs it receives to the Attorney General's Office. The Attorney General's office subsequently opens and oversees the criminal investigation. The Venezuelan constitution guarantees the right to bank privacy and confidentiality, but in cases under investigation by the UNIF, the SBIF, the Attorney General's office, a judge can waive these rights, making Venezuela one of least restrictive countries in Latin America from an investigatory standpoint.

Prior to the passage of the 2005 Organic Law against Organized Crime, there was no special prosecutorial unit for the prosecution of money laundering cases under the Attorney General's office, which is the only entity legally capable of initiating money laundering investigations. As a result of the limited resources and expertise of the drug prosecutors who previously handled money laundering investigations, there have only been three money laundering convictions in Venezuela since 1993, and all of them were narcotics-related. Under the Organic Law against Organized Crime, a new unit is supposed to be established, the General Commission against Organized Crime, with specialized technical expertise in the analysis and investigation of money laundering and other financial crimes. This commission has not been established to date. The Organic Law against Organized Crime also expanded Venezuela's mechanisms for freezing assets tied to illicit activities. A prosecutor may now solicit judicial permission to freeze or block accounts in the investigation of any crime included under the law. However, to date there have been no significant seizures of assets or successful money laundering prosecutions as a result of the law's passage.

The 2005 Organic Law against Organized Crime counts terrorism as a crime against public order and defines some terrorist activities. The law also establishes punishments for terrorism of up to 20 years in prison. However, the Organic Law against Organized Crime does not establish terrorist financing as a separate crime, nor does it provide adequate mechanisms for freezing terrorist assets.

The UNIF has been a member of the Egmont Group since 1999 and has signed bilateral information exchange agreements with counterparts worldwide. Venezuela participates in the Organization of American States Inter-American Commission on Drug Abuse Control (OAS/CICAD) Money Laundering Experts Working Group and is a member of the Caribbean Financial Action Task Force (CFATF). The GOV is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, the UN International Convention for the Suppression of the Financing of Terrorism, and the OAS Inter-American Convention Against Terrorism, and has signed, but not yet ratified, the UN Convention against Corruption. The GOV continues to share money laundering information with U.S. law enforcement authorities under the 1990 Agreement Regarding Cooperation in the Prevention and Control of Money Laundering Arising from Illicit Trafficking in Narcotics Drugs and Psychotropic Substances, which entered into force on January 1, 1991. Venezuela also has a Mutual Legal Assistance Treaty (MLAT) with the United States, which entered into force in March 2004.

The Government of Venezuela took several steps to expand its anti-money laundering regime in 2006 with the implementation of the 2005 Organic Law against Organized Crime. The enactment of this bill has provided law enforcement and judicial authorities the much-needed tools for the effective investigation and prosecution of money laundering derived from all serious crimes, broadened asset forfeiture and sharing provisions, strengthened due diligence requirements, strengthened the capabilities of the Public Ministry to successfully investigate and prosecute crimes related to money laundering, and expanded the mandate of UNIF. However, the deletion of those portions of the proposed law that would have made the UNIF autonomous undercut the credibility and effectiveness

of the unit. Venezuela should also create and enact legislation to criminalize the financing of terrorism, as well as institute measures to expedite the freezing of terrorist assets. Although the passage of the Organic Law against Organized Crime indicates an increased willingness to strengthen the GOV's abilities to fight money laundering, legislation criminalizing the financing of terrorism and allowing for the freezing of terrorist assets is necessary to bring Venezuela into compliance with international standards for combating financial crimes. However, without the political will to implement its anti-money laundering regime, "paper" enhancements to its regime will be ineffective.

Vietnam

Vietnam is not an important regional financial center. Vietnam remains a largely cash-based economy and both U.S. dollars and gold are widely used as a store of value and means of exchange. Real estate prices are commonly quited in gold. Remittances are a large source of foreign exchange, exceeding annual disbursements of development assistance and rivaling foreign direct investment in size. Remittances from the proceeds of narcotics in Canada and the United States are also a source of money laundering as are proceeds attributed to Vietnam's role as a transit country for narcotics.

The Vietnamese banking sector is in the opening phase a transition from a state-owned to a partially privatized industry. At present, approximately 80 percent of the assets of the banking system are held by state-owned commercial banks which allocate much of the available credit to state-owned enterprises. Almost all trade and investment receipts and expenditures are processed by the banking system, but neither trade nor investment transactions are monitored effectively. As a result, the banking system could be used for money laundering either through over or under invoicing exports or imports or through phony investment transactions. Official inward remittances in the first six months of 2006 were estimated to be approximately $2 billion. These amounts are generally transmitted by wire services and while officially recorded, there is no reliable information on either the source or the recipients of these funds. Financial industry experts believe that actual remittances may be double the official figures. There is evidence that large amounts of cash are hand carried into Vietnam, which is legal as long as the funds are declared. The GVN does not require any explanation of the source or intended use of funds brought into the country in this way.

The U.S. Drug Enforcement Agency (DEA) is engaged in a number of investigations targeting significant ecstasy and marijuana trafficking organizations, composed primarily of Vietnamese legal permanent residents in the United States and Vietnamese landed immigrants in Canada as well as naturalized U.S. and Canadian citizens. These drug trafficking networks are capable of laundering tens of millions of dollars per month back to Vietnam, exploiting U.S. financial institutions to wire or transfer money to Vietnamese bank and remittance accounts, as well as engaging in the smuggling of bulk amounts of U.S. currency and gold into Vietnam. The drug investigations have also identified multiple United States-based money remittances businesses that have remitted over $100 million annually to Vietnam. It is suspected that the vast amount of that money is derived from criminal activity. Law enforcement agencies in Australia and the United Kingdom have also tracked large transfers of drug profits back to Vietnam.

Article 251 of the Amended Penal Code criminalizes money laundering. The Counter-Narcotics Law, which took effect June 1, 2001, makes two narrow references to money laundering in relation to drug offenses: it prohibits the "legalizing" (i.e., laundering) of monies and/or property acquired by committing drug offenses (article 3.5); and, it gives the Ministry of Public Security's specialized counter narcotics agency the authority to require disclosure of financial and banking records when there is a suspected violation of the law. The Penal Code governs money laundering related offenses.

In June 2005, GVN issued Decree 74/2005/ND-CP on Prevention and Combating of Money Laundering. The Decree covers acts committed by individuals or organizations to legitimize money or property acquired from criminal activities. The Decree applies to banks and nonbanking financial

institutions. The State Bank of Vietnam (SBV) and the Ministry of Public Security (MPS) take primary responsibility for preventing and combating money laundering. The decree does not cover counterterrorist finance.

SBV supervises and examines financial institutions for compliance with anti-money laundering/counter terrorist financing regulations. Financial institutions are responsible for knowing and recording the identity of their customers. They are required to report cash transactions conducted in one day with aggregate value of VND 200 million (approximately $13,000) or more, or equivalent amount in foreign currency or gold. The threshold for savings transactions is VND 500 million (approximately $31,000). Furthermore, financial institutions are required to report all suspicious transactions. Banks are also required to maintain records for seven years or more. Banks are responsible for keeping information on their customers' secret, but they are required to provide necessary information to law enforcement agencies for investigation purposes.

Foreign currency (including notes, coins and traveler's checks) in excess of $7,000 and gold of more than 300 grams must be declared at customs upon arrival and departure. There is no limitation on either the export or import of U.S. dollars or other foreign currency provided that all currency in excess of $7,000 (or its equivalent in other foreign currencies) is declared upon arrival and departure, and supported by appropriate documentation. If excess cash is not declared, it is confiscated at the port of entry/exit and the passenger may be fined.

The 2005 Decree on Prevention and Combating of Money Laundering provides for provisional measures to be applied to prevent and combat money laundering. Those measures include 1) suspending transactions; 2) blocking accounts; 3) sealing or seizing property; 4) seizing violators of the law; and, 5) taking other preventive measures allowed under the law.

The 2005 Decree also provides for the establishment of an Anti-Money Laundering Information Center under the State Bank of Vietnam (SBV). Similar to a Financial Intelligence Unit (FIU), the Center will function as the sole body to receive and process information. It will have the right to request concerned agencies to provide information and records for suspected transactions. This center was formally established and began operations since February 2006. The Director of the center is appointed by the Governor of the SBV and reports directly to the Governor on anti-money laundering issues. SBV acts as the sole agency responsible for negotiating, concluding and implementing international treaties and agreements on exchange of information on transactions related to money laundering.

The Anti-Money Laundering Information Center will have a separate office with equipment and computers funded by a loan from French Development Assistance. The Center has five full time staff members. Since the Center became operational, it has not detected any suspicious activity.

The MPS is responsible for investigating money laundering related offences. There is no information on investigations, arrests, and prosecutions for money laundering or terrorist financing. MPS is responsible for negotiating and concluding international treaties on judicial assistance, cooperation and extradition in the prevention and combat of money laundering related offenses.

Vietnam is a party to the 1999 International Convention for the Suppression of the Financing of Terrorism. Reportedly, Vietnam plans to draft separate legislation governing counter terrorist financing, though it will not set a specific time frame for this drafting. Currently SBV circulates to its financial institutions the list of individuals and entities that have been included on the UN 1267 Sanctions Committee's consolidated list. No related assets have been identified.

Vietnam is a party to the 1988 UN Drug Convention. Under existing Vietnamese legislation, there are provisions for seizing assets linked to drug trafficking. In the course of its drug investigations, MPS has seized vehicles, property and cash, though the seizures are usually directly linked to drug crimes.

Final confiscation requires a court finding. Reportedly, MPS can notify a bank that an account is "seized" and that is sufficient to have the account frozen.

Vietnam has signed but not ratified the UN Convention against Corruption and is ranked 111 out of 163 countries in Transparency International's 2006 Corruption Perception Index. The Government of Vietnam should promulgate all necessary regulations to fully implement the 2005 decree on the Prevention and Combating of Money Laundering. Vietnam should also pass legislation governing the prevention and suppression of terrorism financing. Vietnam should ratify the UN Conventions against Transnational Organized Crime and Corruption. Vietnamese law enforcement authorities should investigate money laundering, trade fraud, alternative remittance systems, and other financial crimes in Vietnam's shadow economy. Vietnam should become a member of the Asia/Pacific Group on Money Laundering and take additional steps to establish an anti-money laundering/counterterrorist financing regime that comports with international standards.

Yemen

The Yemeni financial system is not yet well developed and the extent of money laundering is not known. Although financial institutions are technically subject to limited monitoring by the Central Bank of Yemen (CBY), alternative remittance systems, such as hawala, in practice, are not subject to scrutiny and are vulnerable to money laundering. The banking sector is relatively small with 17 commercial banks, including four Islamic banks. The CBY supervises the banks. Local banks account for approximately 62 percent of the total banking activities, while foreign banks cover the other 38 percent.

Yemen's parliament passed a comprehensive anti-money laundering legislation (Law 35) in April 2003. The legislation criminalizes money laundering for a wide range of crimes, including narcotics offenses, kidnapping, embezzlement, bribery, fraud, tax evasion, illegal arms trading, and monetary theft, and imposes penalties of three to five years of imprisonment. Yemen has no specific legislation relating to terrorist financing, although terrorism is covered in various pieces of legislation that treat terrorism and terrorist financing as serious crimes.

Law 35 requires banks, financial institutions, and precious commodity dealers to verify the identity of individuals and entities that open accounts (or in the case of the dealers for those who execute a commercial transaction), to keep records of transactions for up to ten years, and to report suspicious transactions. In addition, the law requires that reports be submitted to the Anti-Money Laundering Information Unit (AMLIU), an information-gathering unit within the CBY. This unit acts as the financial intelligence unit (FIU), which in turn reports to the Anti-Money Laundering Committee (AMLC) within the CBY.

The AMLIU is understaffed with a total of three employees at the main office. The 18 field inspectors for banking supervision also serve as investigators for the AMLIU. The AMLIU has no database and is not networked internally or to the rest of the CBY. The CBY provides training to other members of the government to assist in elements of anti-money laundering enforcement, but the lack of capacity hampers any attempts by the AMLIU to control illicit activity in the formal financial sector.

The AMLC is composed of representatives from the Ministries of Finance, Foreign Affairs, Justice, Interior, and Industry and Trade, the Central Accounting Office, the General Union of Chambers of Commerce and Industry, the CBY, and the Association of Banks. The AMLC is authorized to issue regulations and guidelines and provide training workshops related to combating money laundering efforts.

Law 35 also grants the AMLC the right to exchange information with foreign entities that have a signed a letter of understanding with Yemen. The head of the AMLC is empowered by law to ask local judicial authorities to enforce foreign court verdicts based on reciprocity. Also, the law permits

the extradition of non-Yemeni criminals in accordance with international treaties or bilateral agreements.

Prior to passage of the anti-money laundering law, the CBY issued Circular 22008 in April 2002, instructing banks and financial institutions that they must verify the legality of all proceeds deposited in or passing through the Yemeni banking system. The circular stipulates that financial institutions must positively identify the place of residence of all persons and businesses that establish relationships with them. The circular also requires that banks verify the identity of persons or entities that wish to transfer more than $10,000, when they have no accounts at the banks in question. The same provision applies to beneficiaries of such transfers. The circular also prohibits the transfer of more than $10,000 cash in or out of the country without prior permission from the CBY, although this requirement is not strictly enforced. Banks must also take every precaution when transactions appear suspicious, and report such activities to the AMLIU. The circular has been distributed to the banks along with a copy of the Basel Committee's "Customer Due Diligence for Banks," concerning "know your customer" procedures and "Core Principles for Effective Banking Supervision". The CBY issued Circular No. 4 on December 9, 2003, ordering banks to set up intelligence gathering units specializing in investigating and monitoring suspicious funds and transactions in their regulatory structures. In 2006, however, no reports of suspicious type activity were filed with the AMLIU, and there were no prosecutions.

In September 2003, the CBY responded to the UNSCR 1267 Sanctions Committee's consolidated list, the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224, and Yemen's Council of Ministers' directives, by issuing two circulars (75304 and 75305) to all banks operating in Yemen. Circulars 75304 and 75305 directed banks to freeze the accounts of 144 persons, companies, and organizations, and to report any findings to the CBY. As a result, one account was immediately frozen. Circular No. 75304 also contained a consolidated list of all persons and entities belonging to al-Qaida (182) and the Taliban (153). In 2006, the CBY began issuing a circular every three months containing an updated list of persons and entities belonging to al-Qaida and the Taliban. Since the February 2004 addition of Sheikh Abdul Majid Zindani to the UNSCR 1267 Sanctions Committee's consolidated list, the Yemeni government has made no known attempt to enforce the sanctions and freeze his assets.

A law was passed in 2001 governing charitable organizations. This law entrusts the Ministry of Labor and Social Affairs with overseeing their activities. The law also imposes penalties of fines and/or imprisonment on any society or its members convicted of carrying out activities or spending funds for other than the stated purpose for which the society in question was established. The CBY Circular No. 33989 of June 2002, and Circular No. 91737 of November 2004, ordered banks to abide by the enhanced controls regulating the opening and management of the accounts of charities. This was in addition to keeping these accounts under continuous supervision in coordination with the Ministry of Labor and Social Affairs.

During 2006, the CBY has been active in educating the public and the financial sector, including money services businesses and money laundering reporting officers, about the proper ways and means of detecting and reporting suspicious financial transactions. They have done so through public forums and workshops. In 2005, the AMLC distributed an anti-money laundering procedural directory to all public and private financial institutions. The directory explains how to monitor and report suspected money laundering cases.

Yemen is one of the original signatories of the memorandum of understanding governing the establishment of the Middle East and North Africa Financial Action Task Force (MENAFATF). Yemen is a party to the 1988 UN Drug Convention, and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Yemen is a party to the Arab Convention for the Suppression of Terrorism.

Yemen has a large underground economy. The smuggling of trade goods and contraband are profitable. The use of khat is common in Yemen and there have been a number of investigations over the years of khat being smuggled from Yemen and East Africa into the United States and profits laundered and repatriated via hawala networks. Yemen is rated 119 out of 163 countries in Transparency International's 2006 Corruption Perception Index.

The Government of Yemen (GOY) should continue to develop an anti-money laundering regime that adheres to international standards, including the FATF recommendations. In particular, banks and nonbank financial institutions should enhance their capacity to detect suspicious financial transactions and should report such transactions to a strengthened AMLIU for analysis and possible investigation by Yemeni law enforcement. Yemen should examine the prevalence of alternative remittance systems such as hawala and how the hawala networks are used in money laundering and value transfer. Law enforcement and customs authorities should also examine trade-based money laundering and customs fraud. As a next step, Yemen should enact specific legislation with respect to terrorist financing and forfeiture of the assets of those suspected of terrorism. Yemen should ratify the UN Convention against Transnational Organized Crime and should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism. Yemen should enforce the sanctions and freeze the assets of Sheikh Abdul Majid Zindani who was added to the UN 1267 Sanctions Committee Consolidated list in February 2004.

Zimbabwe

Zimbabwe is not a regional financial center, but as the pace of economic contraction accelerates, it faces a serious, growing problem with official corruption and other risk factors associated with money laundering, such as a flourishing parallel exchange market; widespread evasion of exchange controls by legitimate businesses; and company ownership through nominees. Deficiencies in the Government of Zimbabwe's (GOZ) regulatory and enforcement framework contribute to Zimbabwe's potential as a money laundering destination. These deficiencies include: an increasingly understaffed bank supervisory authority; a lack of trained regulators and lack of investigators to investigate and enforce violations and financial crime; financial institutions determined to bypass the regulatory framework; limited asset seizure authority; a laissez-faire attitude toward compliance with the law on the part of elements of the business community; ready acceptance of the U.S. dollar in transactions and, significant gold exports and illegal gold trading.

In December 2003, the GOZ submitted the "Anti-Money Laundering and Proceeds of Crime Act" to Parliament, which enacted the legislation. This bill criminalized money laundering and implemented a six-year record keeping requirement. In 2004, the GOZ adopted more expansive legislation in the "Bank Use Promotion and Suppression of Money Laundering Act" ("The Act") that extended the anti-money laundering law to all serious offenses. The Act mandated a prison sentence of up to fifteen years for a conviction. It also criminalized terrorist financing and authorized the tracking and seizure of assets. The Act has reportedly raised human rights concerns due to the GOZ's history of selective use of the legal system against its opponents, but its use to date has not been associated with any reported due process abuses or provoked any serious public opposition. The Exchange Control Order, enacted in 1996, obligates banks to require individuals who deposit foreign currency into a foreign currency account to submit a written disclosure of sources of the funds.

The Reserve Bank of Zimbabwe (RBZ) is the lead agency for prosecuting money laundering offenses. In May 2006, the RBZ issued new Anti-Money Laundering Guidelines that outlined and reinforced requirements established in the Act for financial institutions and designated nonfinancial businesses and professions. These binding requirements make provisions regarding politically exposed persons and include the obligation to gather and make available to regulators more personal data on these high-profile clients. Financial institutions must now keep records of accounts and transactions for at least

ten years, and report any suspicious transactions to the financial intelligence unit (FIU). The Act also criminalizes tipping off. Failure to report suspected money laundering activities carries a possible fine of Z$5 million (approximately $20,000), and violating rules on properly maintaining customer data carries a possible fine of Z$1 million (approximately $4,000).

The 2004 Act provides for the establishment of an FIU. The Financial Intelligence Inspectorate and Evaluation Unit (FIIE) is housed within the RBZ. The FIIE receives suspicious transaction reports (STRs), issues guidelines such as those issued in May 2006, and enforces compliance with procedures and reporting standards for obligated entities.

According to the Governor of the RBZ, the GOZ has been working throughout 2006 on legislation to address problems with cybersecurity and cybercrime, including money laundering via electronic means. However, the legislation has not been passed. During the year, the RBZ sharpened limits on daily cash withdrawals for individuals and companies, ostensibly in an effort to curtail money laundering but more likely to inhibit private sector parallel foreign exchange activities. In November, the Zimbabwe dollar was trading on the parallel market at a historic premium of about 700 percent above the official exchange rate. The central bank began monitoring all payments by financial institutions of more than Z$1 million (approximately $4,000 at the official exchange rate). When requested, the local banking community has cooperated with the GOZ in the enforcement of asset tracking laws. However, increasingly burdensome GOZ regulations and the resulting hostile business climate have led to growing circumvention of the law by otherwise legitimate businesses.

The GOZ continued to arrest prominent Zimbabweans for activities that it calls “financial crimes.” Prosecutions for such crimes, however, have reportedly been selective and politically motivated. The government often targets persons who have either fallen out of favor with the ruling party, or individuals without high-level political backing. To date, the Act has not been employed in the prosecution of individuals for such offenses. The GOZ prefers to prosecute financial crimes under the Criminal Procedures and Evidence Act, rather than the Anti-Money Laundering Act, because it allows for those charged to be held in custody for up to 28 days. During the year, the authorities made two high-profile arrests of persons (both Nigerian nationals) attempting to smuggle significant sums of foreign currency out of the country.

Most of these crimes involved violations of currency restrictions that criminalize the externalization of foreign exchange. In light of the inability of the vast majority of businesses to access foreign exchange from the RBZ, most companies privately admit to externalizing their foreign exchange earnings or to accessing foreign currency on the parallel market. Moreover, the GOZ itself, through the RBZ, has been a major purchaser of foreign currency on the parallel market. Citing “nonperformance and defiant behavior by most players” in the money transfer sector, in October the RBZ canceled the licenses of all money transfer agencies (MTAs). The MTAs reportedly were exchanging foreign currency at the parallel market rate. Many observers speculated this move would fuel an even greater use of already popular alternative remittance systems.

In August, the GOZ implemented a currency re-denomination program that slashed three zeros from Zimbabwe’s currency (so that Z$100,000 became Z$100). The purpose of the campaign was to assert greater GOZ control over the financial sector and to attempt to reassure a public concerned about the 1200 percent inflation within their country. The RBZ gave all holders of the old currency 21 working days to deposit their cash holdings into the banking system, and set limits for cash deposits either without proof of the source of funds, or without depositors being interrogated on the origins of their money. Although the campaign had nothing to do with cracking down on money laundering, when the holder of cash could not prove a legitimate source of funds, the cash was deposited into zero-interest “anti-money laundering coupons,” and the case was referred to the RBZ’s Suppression of Money Laundering Unit for further investigation. To evade these requirements, those with an excess of cash, such as entrepreneurs, have purchased high-value commodities to retain their wealth. During the

changeover period, there were numerous reports of police arbitrarily seizing cash without issuing receipts or filing official documentation with the authorities. The government claimed that more than 2,000 persons were arrested for "money laundering" in this period and charged under the Exchange Control Act. The government has not provided any additional information about the status or resolution of any of these cases.

The 2001 Serious Offenses (Confiscation of Profits) Act establishes a protocol for asset forfeiture. The Attorney-General may request confiscation of illicit assets. The Attorney-General must apply to the court that has rendered the conviction within six months of the conviction date. The court can then issue a forfeiture order against any property. Despite the early date of this law compared to the money laundering legislation that followed, this law does define and incorporate money laundering among the bases for the GOZ to confiscate assets.

With the country in economic collapse and increasingly isolated, Zimbabwe's laws and regulations remained ineffective in combating money laundering. The May 2006 guidelines notwithstanding, the government's anti-money laundering efforts throughout the year appeared to be directed more at securing the government's own access to foreign currency than to ensuring compliance. Despite having the legal framework in place to combat money laundering, the sharp contraction of the economy, growing vulnerability of the population, and decline of judicial independence raise concerns about the capacity and integrity of Zimbabwean law enforcement. The banking community and the RBZ have cooperated with the United States in global efforts to identify individuals and organizations associated with terrorist financing.

Zimbabwe is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime or the African Union Anti-Corruption Convention. Zimbabwe has yet to sign the UN International Convention for the Suppression of the Financing of Terrorism. Zimbabwe joined the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) in 2003 and in August 2006, assumed the Presidency for ESAAMLG for the 2006/2007 administrative year.

Transparency International ranks the Government of Zimbabwe at 130 of 163 countries on its Corruption Perception Index. The GOZ leadership should work to develop and maintain transparency, prevent corruption, and to subscribe to practices ensuring the rule of law. The GOZ must also work toward reducing the rate of inflation, halting the financial collapse, and rebuilding the economy to restore confidence in the currency. The GOZ can illustrate its seriousness in combating money laundering and terrorism financing by using its legislation for the purposes for which it was designed, instead of using it to persecute opponents of the regime and nongovernmental organizations with which it opposes. Once these basic prerequisites are met, the GOZ should endeavor to develop and implement an anti-money laundering/counterterrorist regime that comports with international standards.