

# **International Narcotics Control Strategy Report**

Released by the Bureau for International Narcotics and Law Enforcement Affairs  
March 2005

## **Country Reports: N-Z**

### **Namibia**

Namibia is not a regional financial center. In addition to its Central Bank, Namibia has four commercial banks. Of particular concern in Namibia is the smuggling of precious minerals and gems, the proceeds of which Namibian authorities think may be laundered through Namibian financial institutions.

In November of 2004, Namibia criminalized money laundering with passage of the Prevention of Organized Crime Bill. The new law requires both bank and non-bank financial institutions to report suspicious transactions to the Central Bank and provide relevant documents and other information to government authorities for use in criminal investigations. Non-bank financial institutions, such as private pension funds, the stock exchange, and investment companies, were previously exempted from such reporting requirements.

Parliament will consider a separate anti-money laundering bill—the Financial Intelligence Act (FIA)—in early 2005. The FIA is expected to add additional reporting requirements and strengthen the Government's ability to investigate and prosecute money laundering crimes. It will also establish a financial intelligence unit. The FIA is also expected to address cross-border currency reporting requirements and information sharing with foreign law enforcement authorities. Namibia currently does not have laws that criminalize the financing of terrorism. The Government intends to table its Combating of Terrorist Activities Bill in Parliament in 2005. Under the proposed counterterrorism law, the Government would be empowered to proscribe an organization if it commits or participates in terrorism; prepares for acts of terrorism; promotes or encourages terrorism; or is otherwise involved with terrorism. The proposed law would also prohibit individuals from providing money or other property with the intention or knowledge (or suspicion) that such money or other property would be used for the purposes of terrorism (regardless whether or not a terrorism act was committed). Individuals who do so would be subject to prosecution and imprisonment not to exceed 20 years. There have been no known arrests or prosecutions for money laundering or terrorist financing since January 1, 2004.

Namibia is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG). Namibia served as the Chair of ESAAMLG from August 2001 until August 2002. Namibia is a party to the UN Convention against Transnational Organized Crime and the 1988 UN Drug Convention. In November 2001, the GRN signed the UN International Convention for the Suppression of the Financing of Terrorism, and is making progress toward becoming a party.

The Government of Namibia should pass counterterrorism and related legislation that criminalizes terrorism financing and further strengthens the country's nascent anti-money laundering regime, as it has committed to doing through its membership in ESAAMLG. Namibia should continue its efforts toward becoming a party to the UN International Convention for the Suppression of the Financing of Terrorism.

### **Nauru**

Nauru is a small Central Pacific island nation with a population of approximately 13,000. It is an independent republic and an associate member of the British Commonwealth. The Republic of Nauru is an established "zero" tax haven, as it does not levy any income, corporate, capital gains, real estate, inheritance, estate, gift, sales, or stamp taxes. The currently insolvent government-owned Bank of Nauru acts as the Central Bank for monetary policy. Nauru's legal, supervisory, and regulatory framework has provided significant opportunities in the past decade for the laundering of the proceeds of crime.

In June 2000, the Financial Action Task Force (FATF) placed Nauru on its initial list of fifteen Non-Cooperative Countries and Territories. In response to mounting international pressure, the Government of Nauru, in August 2001, passed the Money Laundering and Proceeds of Crime Act of 2001 (AMLA 2001). The AMLA 2001 requires financial institutions to verify and record the identity of account holders and to maintain accounts in the name of the account holder, thereby prohibiting anonymous accounts and accounts held in fictitious names. The AMLA 2001 also requires financial institutions to report suspicious transactions, and to develop internal anti-money laundering policies and procedures. The new legislation allowed for the establishment of a Financial Intelligence Unit (FIU) called the Financial Institutions Supervisory Authority (FISA). FISA has not yet been formed and no suspicious transaction reports have been filed to it. The AMLA 2001 provided for mutual assistance with respect to money laundering investigations. However, there are limitations regarding compliance with foreign requests for assistance. Nauru may refuse to comply with a foreign request if the action sought by the foreign authority is contrary to any provision of the Republic of Nauru Constitution, or would prejudice the national interest. However, the Government of Nauru (GON) has since cooperated with officials from the United States and other countries in certain criminal investigations involving Nauru's institutions.

On September 7, 2001, the FATF issued a press release recognizing the passage of the Nauru's AMLA 2001. The FATF, however, found the legislation to have several deficiencies. It urged Nauru to enact appropriate amendments by November 30, 2001, in order to avoid the application of countermeasures. On December 5, 2001, the FATF called upon its members to impose countermeasures against Nauru because of Nauru's failure to remedy deficiencies in its anti-money laundering regime.

On December 6, 2001, Nauru amended the AMLA 2001 to address certain deficiencies in the original act. The amendment clarified that the law applies to all financial institutions incorporated under the laws of Nauru (as opposed to just financial institutions conducting business within Nauru). It also broadened the definition of money laundering. Despite the passage of its anti-money laundering legislation with amendments, Nauru continued to lack a legal framework and an effective regime for the regulation and supervision of the nearly 400 registered offshore banks.

In January 2002, the U.S. Treasury Department supplemented its previously issued advisory by reminding U.S. banks and other financial institutions of their obligations under the newly enacted Section 313 of the USA PATRIOT Act of 2001 concerning correspondent accounts with foreign shell banks. Under this new law, U.S. financial institutions, as well as other financial institutions operating in the United States, are required to terminate any U.S. correspondent accounts provided to foreign shell banks, and they must take reasonable steps to ensure that correspondent accounts held by foreign banks are not being used to provide U.S. banking services indirectly to foreign shell banks.

In December 2002, the Secretary of Treasury, after consultation with the Departments of Justice and State as well as other concerned U.S. government agencies, designated Nauru as a jurisdiction of "primary money laundering concern" under Section 311 of the USA PATRIOT Act. In the announcement, the U.S. Treasury published a list of 161 banks licensed by the Republic of Nauru, the majority of which were thought to be shell banks. In April 2003, U.S. Treasury and FinCEN issued a proposed rule pursuant to section 311 to invoke Special Measure Five, prohibiting U.S. financial institutions from opening or maintaining any payable-through or correspondent accounts involving a Nauru financial institution.

The Anti-Money Laundering Act 2003 AMLA consolidates the Anti-Money Laundering Act of 2001 and the Anti-Money Laundering (Amendment) Act of 2001. The amended legislation gives the Nauru FIU, the Financial Institutions Supervisory Authority, if and when it is established, authority to cooperate

with foreign states, including the power to obtain search warrants, track property, and issue monitoring orders. The amended legislation also gives the Director of Public Prosecutions the power to freeze and seize assets relating to money laundering. Legislative amendments to the Corporation Act 1972 were also enacted in 2003 to abolish offshore banking and eliminate all bank secrecy provisions. Nauru took further steps to publish the list of corporations that recently held Nauruan offshore banking licenses.

Following the election of a reformist government in 2004, Nauru enacted a series of legislative acts to reform its anti-money laundering laws and respond to deficiencies identified by the FATF. In 2004, the GON passed the Anti-Money Laundering Act of 2004, the Banking (Amendment) Act of 2004, the Corporation (Amended) Act of 2004, the Financial Transactions Reporting Act of 2004, the Counter-Terrorism and Transnational Organized Crime Act of 2004, the Mutual Assistance in Criminal Matters Act of 2004, and the Proceeds of Crime Act 2004.

The Anti-Money Laundering Act 2004 enacted on September 6, 2004 expands the coverage and scope of anti-money laundering requirements to banks, money remitters, securities and investment businesses, insurance, real estate agents, dealers in precious metals and stones, trust or company service providers, and legal entities. The new legislation provides the powers of search and seizure to law enforcement, and enables freezing and forfeiture of tainted property and terrorist property. The Act also allows mutual assistance in relation to anti-money laundering investigations with foreign states.

At the October 2004 Plenary, the FATF recommended that its member states withdraw all countermeasures against Nauru in view of Nauru's having taken several significant steps to ensure that offshore banks previously licensed in Nauru no longer existed and no longer conducted banking activity. As of January 1, 2005, The United States had not conformed to the FATF recommendation to withdraw its countermeasure. The FATF also invited Nauru to submit an implementation plan with benchmarks and timetables regarding the steps it would take to cure the remaining deficiencies of its anti-money laundering regime.

A technical team from the Pacific Island Forum Secretariat (PIF) will travel to Nauru in early 2005 to assist Nauru in developing and implementing its anti-money laundering regime. The PIF technical team will assist in establishing Nauru's FIU- the Financial Institutions Supervisory Authority- and will provide training for prosecutors and investigators of financial crimes.

Nauru has observer status within the Asia/Pacific Group on Money Laundering and recently joined the United Nations. Nauru has signed, but not yet ratified, the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime.

The Government of Nauru should continue to work with the Financial Action Task Force (FATF) to ensure that its anti-money laundering regime comports with the FATF's revised Forty Recommendations and its nine Special Recommendations on Terrorist Financing, and that whatever remnant of its offshore financial sector remains is regulated consonant with those standards. Nauru should become a party to the UN International Convention for the Suppression of the Financing of Terrorism, and to all UN Conventions pertaining to terrorism. Nauru should also ratify the UN Convention against Transnational Crime and accede to the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.

## **Nepal**

Nepal is not a regional financial center and there are no indications that Nepal is used as an international money laundering center. The Government of Nepal (GON) has not criminalized money laundering, and legislation on money laundering, mutual legal assistance and witness protection, developed as part of the GON's Master Plan for Drug Abuse Control, remained stalled in 2004. Since the dissolution of Parliament in May 2002, any new laws must be passed by royal ordinance, which must be renewed after six months. Draft anti-money laundering legislation has been prepared but has not yet passed into law or ordinance. There were no prosecutions or even arrests for money laundering during 2004.

Banks are required to record the identity of customers engaging in significant transactions. In particular, all transactions which involve payments in foreign currency require prior approval by the NRB (Nepal's Central Bank). Any Nepali citizen who wishes to open a foreign currency account must obtain a license to do so from the NRB, and Nepali citizens wishing to take currency overseas must obtain approval from the NRB by clearly outlining the purpose for transferring funds overseas. The NRB normally approves small amounts (in USD thousands) for travel, education and medical treatment. For business transactions, however, a letter of credit from a bank recognized by the NRB must be opened by documenting the transaction details. Banks have provided records regarding bank accounts of individuals and institutions to assist in GON investigations into corruption by senior officials. Nepal has enacted bank secrecy laws that prevent the disclosure of client and ownership information to individuals and law enforcement authorities; however, the present law does not prevent the disclosure of client and ownership information to the NRB, courts, auditors or the Commission for Investigation of Abuse of Authority (CIAA). Nepal has explored the development of an offshore financial sector, but one does not exist at present.

The NRB has the authority to freeze and seize assets related to criminal investigations. However, the GON's ability to identify and trace assets is hindered by a lack of a computerized information sharing system. For example, many bank branch offices do not have computers. The Nepal Police also have the authority to seize any goods or property related to criminal investigations.

A hawala system of informal remittances (called the hundi system in Nepal) is widespread. Expatriate Nepali workers—the primary source of hundi transactions—are often employed in the Gulf, Malaysia, and other countries that have introduced new, more stringent regulations on informal remittance systems. Nepali workers in India still utilize hawala-hundi transactions. There have been no significant initiatives to regulate the system in Nepal. However, GON officials claim that changes in the laws of other countries have forced some Nepalese hundi users to conduct their transactions through formal banking institutions. In Nepal, the hundi system is linked to issues of capital flight, tax avoidance, and corruption.

Nepal has not passed any laws criminalizing terrorist financing. However, the Terrorist and Destructive Activities Act and the Bank and Financial Institutions Ordinance 2004, working in tandem, reportedly criminalize terrorist financing. Under the Bank and Financial Institutions Ordinance 2004, the NRB has the authority to seize any assets deemed to have been used in terrorist activities. No assets belonging to individuals or entities on the UNSCR 1267 Sanctions Committee's consolidated list have been identified in Nepal. Additionally, the State Offense Act of 1989 authorizes security forces to arrest and prosecute any Nepalese or foreign citizen involved in any criminal activities against the state or associated with foreign terrorist activity. The GON made one arrest for terrorist financing in 2004.

The Government of Nepal is a party to the 1988 UN Drug Convention. It has also signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Nepal should proceed with ratification of this Convention. Nepal should also sign and ratify the UN International Convention for the Suppression of the Financing of Terrorism. Legislative action in Nepal has clearly been handicapped by the lack of a sitting Parliament. As soon as practicable, Nepal should enact the provisions of its 2002 Master Plan for Drug Control, including anti-money laundering and terrorist finance legislation, and develop a comprehensive anti-money laundering regime that would require the mandatory filing of suspicious transaction reports (and clarify that this may be done without violating current bank secrecy provisions), foster international cooperation in the area of anti-money laundering initiatives, and establish a financial intelligence unit. It also should initiate efforts to regulate its domestic hundi dealers.

## **The Netherlands**

The Netherlands is a major financial center and as such is an attractive target for the laundering of funds generated from a variety of illicit activities. Activities involving money laundering are often related to the sale of heroin, cocaine, cannabis, or synthetic and designer drugs (such as ecstasy). Activities involving financial fraud are believed to generate a considerable portion of domestic money laundering. Much of the money laundered in the Netherlands is likely owned by major drug cartels and other international criminal organizations and much of it flows through the formal financial sector. There are no indications of syndicate-type structures in organized crime or money laundering, and

there is virtually no black market for smuggled goods in the Netherlands. Although under the Schengen Accord there are no formal controls on the borders with Germany and Belgium, the Dutch authorities run special operations in the border areas designed to keep smuggling to a minimum. The Netherlands is not an offshore financial center nor are there any free trade zones in the Netherlands.

In 1994, the Government of the Netherlands (GON) criminalized money laundering related to all crimes, although prosecutors first had to prove the predicate offense before prosecuting for money laundering. In December 2001, legislation was enacted making facilitating, encouraging, or engaging in money laundering a separate criminal offense, regardless of the source of the funds, easing somewhat the government's burden of proof regarding the criminal origins of proceeds. Under the law, the GON needs only to prove that the proceeds "apparently" originated from a crime; self-laundering is also covered. The penalty for deliberate acts of money laundering is a maximum of four years' imprisonment and a maximum fine of 45,000 euros, while liable acts of money laundering (of people who do not know first-hand of the criminal nature of the origin of the money, but should have reason to suspect it) are subject to a maximum imprisonment of one year and a fine no greater than 45,000 euros. Repeated convictions for money laundering offenses may be punished with a maximum imprisonment of six years and a maximum fine of 45,000 euros, and those convicted may also have their professional licenses revoked. In addition to criminal prosecution for money laundering offenses, money laundering suspects can also be charged with participation in a criminal organization (Article 140 of the Penal Code), violations of the financial regulatory acts, violations of the Sanctions Act, or noncompliance with the obligation to declare unusual transactions according to the Economic Offenses Act.

The Netherlands has comprehensive money laundering legislation. The Services Identification Act (WID) and the Disclosure Act set forth identification and reporting requirements. All financial institutions in the Netherlands, including banks, bureaux de change, casinos, life insurance companies, securities firms, stock brokers, and credit card companies, are required to report cash transactions over 15,000 euros, as well as any less substantial transaction that appears unusual, a broader standard than "suspicious" transactions, to the Office for Disclosure of Unusual Transactions (MOT), the Netherlands' Financial Intelligence Unit (FIU). In December 2001, the reporting requirements were expanded to include trust companies, financing companies, and commercial dealers of high-value goods. In June 2003, notaries, lawyers, real estate agents/intermediaries, accountants, business economic consultants, independent legal advisers, trust companies and other providers of trust related services, and tax advisors were added. Reporting entities that fail to file reports with the MOT may be fined 11,250 euros or be imprisoned up to two years. Under the Identification of Services Act (WID), all those that are subject to reporting obligations must identify their clients, including the identity of ultimate beneficial owners, either at the time of the transaction or at some point prior to the transaction, before providing financial services.

Financial institutions are also required by law to maintain records necessary to reconstruct financial transactions for at least seven years. The requirements also have been applicable to the Central Bank of the Netherlands (to the extent that it provides covered services) since 1998. There are no secrecy laws or fiscal regulations that prohibit Dutch banks from disclosing client and owner information to bank supervisors, law enforcement officials, or tax authorities. Financial institutions and all other institutions under the reporting and identification acts, and their employees, are specifically protected by law from criminal or civil liability related to cooperation with law enforcement or bank supervisory authorities. Furthermore, current legislation requires Customs authorities to report unusual transactions to the MOT; however, the Dutch do not currently have a currency declaration requirement for incoming travelers.

The Money Transfer and Exchange Offices Act, which was passed in June 2001, requires money transfer offices, as well as exchange offices, to obtain a permit to operate, and subjects them to supervision by the Central Bank. Every money transfer client has to be identified.

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

The MOT, which was established in 1994, reviews and analyzes the unusual transactions and cash transactions filed by banks and financial institutions. The MOT receives over 85 percent of unusual transaction reports electronically through its secure website. It forwards suspicious transaction reports with preliminary investigative information to the Police Investigation Service and to the office for operational support of the National Public Prosecutor for MOT cases (BLOM). In 2002, the MOT received 137,339 reports and forwarded 24,741 to the BLOM as suspicious transactions. In 2003, the MOT received 177,157 unusual reports (totaling over 1.5 billion euros), of which 37,748 were flagged by the MOT as suspicious transactions for further investigation by the BLOM. The 30 percent increase in reports is attributed to the new reporting requirements for money transfer businesses and high value goods dealers as well as an increase in the total amount of money transfers. The average amount reported was 41,000 euros in 2003, an increase from the 34,800 euros reported (on average) in 2002.

In order to facilitate the forwarding of suspicious transactions, the MOT and BLOM created an electronic network called Intranet Suspicious Transactions (IST). Also, a secure website for the actual reporting of unusual transactions by financial institutions was developed, thus completing the electronic infrastructure. Furthermore, fully automatic matches of data with the police databases are included with the unusual transaction reports forwarded to the BLOM. Since the money laundering detection system also covers areas outside the financial sector, the system is used for detecting and tracing terrorist financing activity.

On January 1, 2003, the MOT and BLOM formed a special unit (the MBA-unit) to work together to analyze data generated from the IST. Once the data is analyzed by the MBA-unit, it forwards reports to the police. In 2003, the MBA-unit sent 275 reports to the police for further investigations. Future plans are for the MBA-unit to focus on more project-based strategic type work by analyzing transaction reports that fit profiles provided by the police.

In 2003, BLOM opened 559 investigations, which involved 13,171 transactions. Of these 559 investigations, 75 were related to actions by the Public Prosecutor Hit-And-Run Money Laundering (HARM) team, established in 2001, resulting in the confiscation of approximately 8.1 million euros and the arrest of 78 suspects. Both the MOT and BLOM are internationally recognized institutions that play a major role in the Egmont Group. BLOM provides the anti-money laundering division of Europol with suspicious transaction reports, and Europol applies the same analysis tools as BLOM.

In 2004, an evaluation of the anti-money laundering reporting system, commissioned by the Minister of Justice, was published. In response to the report, the GON announced a number of measures to enhance the effectiveness of the anti-money laundering system. These measures include: an instruction on money laundering for the Public Prosecution Service, new indicators for reporting requirements, amendments to anti-money laundering legislation (Disclosure Act and the Identification of Services Act), and an agreement of cooperation between the National Police and the Dutch Internal Revenue Service Investigation Office. These measures are currently being implemented or will take effect during the course of 2005.

The Netherlands has enacted legislation governing asset forfeitures. The 1992 Asset Seizure and Confiscation Act enables the authorities to confiscate assets that are illicitly obtained or otherwise connected to criminal acts. The legislation was amended in 2003 to improve and strengthen the options for identifying, freezing, and seizing criminal assets. The police and several special investigation services are responsible for enforcement in this area. These entities have adequate powers and resources to trace and seize assets. Asset seizure has been fully integrated into all law enforcement investigations into serious crime. Statistics provided by the Office of the Public Prosecutor show that the amount of assets seized in 2003 amounted to 10.1 million euros (\$11 million), compared to 7.9 million euros (\$10.5 million) in 2002. The United States and the Netherlands have an agreement on asset sharing dating back to 1994. The Netherlands also has a treaty on asset sharing with the UK, as well as an agreement with Luxembourg.

In June 2004, the Minister of Justice sent an evaluation study to the Parliament on specific problems encountered with asset forfeiture in large, complex cases. In response to this report, the GON announced several measures to improve the effectiveness of asset seizure enforcement, including steps to increase expertise in the financial and economic field, assign extra public prosecutors to

improve the coordination and handling of large, complex cases, and establish a specific asset forfeiture fund.

Terrorist financing is a crime in the Netherlands. The "Sanction Provision for the Duty to Report on Terrorism" was passed in 1977 and amended in June 2002, to implement European Union (EU) Regulation 2580/2001 and UNSCR 1373. This ministerial decree provides authority to the Netherlands to identify, freeze, and seize terrorist finance assets. The decree also requires financial institutions to report to the MOT all transactions (actually carried out or intended) that involve persons, groups, and entities that have been linked, either domestically or internationally, with terrorism. Any terrorist crime will automatically qualify as a predicate offense under the Netherlands "all offenses" regime for predicate offenses of money laundering. Involvement in financial transactions with individuals and/or organizations designated nationally, by the EU, or by the UN has been made a criminal offense. The Dutch Finance Ministry, in close coordination with the Foreign Affairs Ministry, distributes lists of designated entities to financial institutions and relevant government bodies (including local tax authorities). Freezing of assets is an administrative procedure. The Netherlands has frozen more terrorist related assets than any other EU member state.

The Act on Terrorist Offenses took effect on August 10, 2004. The new Act introduces Article 140A of the Criminal Code, which criminalizes participation in an organization when the intent is to commit acts of terrorism, and defines participation as membership or providing provision of monetary or other material support. Article 140A carries a maximum penalty of fifteen years' imprisonment for participation in and life imprisonment for leadership of a terrorist organization. The Netherlands Security Service investigates terrorist financing, and is cooperating with law enforcement entities that are experienced in this area.

Dutch civil law requires registration of all active foundations in the registers of the Chambers of Commerce. Each foundation's formal statutes (creation of the foundation must be certified by a notary of law) must be submitted to the Chambers. Charitable institutions also register with, and report to, the tax authorities in order to qualify for favorable tax treatment. Approximately 15,000 organizations (and their managements) are registered in this way. The organizations have to file their statutes, showing their purpose and mode of operations, and submit annual reports. Samples are taken for auditing. Data about informal hawala banking as a potential money laundering/terrorist financing source is still scarce. The Ministry of Justice has ordered a study in this field, to be published shortly.

The Netherlands is in full compliance with all Financial Action Task Force (FATF) Recommendations, with respect to both legislation and enforcement. The Netherlands also complies with the EU Second Money Laundering Directive, and in some areas, is ahead of the EU legislation (such as full money laundering controls on money remitters, including licensing and identification of customers). In December 2003, the International Monetary Fund (IMF) conducted an assessment of the Netherlands' anti-money laundering and counterterrorist financing system. The Report on the Observance of Standards and Codes (ROSC), released in September 2004, indicates that the Netherlands has a sound anti-money laundering and counterterrorist financing framework.

In December 2004, the Dutch EU Presidency reached a political agreement within the EU on the Third Money Laundering Directive. The Dutch have already implemented some obligations resulting from this directive, such as effective supervision of currency exchange offices and trust companies. In November 2004, the Dutch EU Presidency also reached political agreement within the EU on a regulation controlling cross-border cash movements.

The MOT supervised the PHARE Project for the European Union (March 2002-December 2003). The PHARE Project was the European Commission's Anti-Money Laundering Project for Economic Reconstruction Assistance to Estonia, Latvia, Lithuania, Poland, the Czech Republic, Slovakia, Hungary, Slovenia, Romania, Bulgaria, Cyprus, and Malta. The purpose of the project was to provide support to Central and Eastern European countries in the development and/or improvement of anti-money laundering regulations. For this purpose, the MOT established a project team and a consortium of international experts. Although the PHARE project concluded in December 2003, the MOT will still move forward with the enhancement of the FIU.NET Project, (an electronic exchange of current information between European FIUs by means of a secure web). Currently, there are eight countries

connected to the FIU.NET in Central and Eastern Europe. A representative of the Dutch MOT is assisting the Surinamese government in establishing a FIU.

The United States enjoys good cooperation with the Netherlands in fighting international crime, including money laundering. In September 2004, the United States and the Netherlands signed two agreements in the area of mutual legal assistance and extradition, stemming from the agreements that were concluded in 2003 between the EU and the United States. One of the amendments to the existing bilateral agreement is the exchange of information on bank accounts. The MOT has established close links with the U.S Treasury's FinCEN and is also involved in efforts to expand international cooperation between disclosure offices.

The Netherlands is a member of the FATF and participates in the Caribbean Financial Action Task Force as a Cooperating and Supporting Nation. The MOT is a member of the Egmont Group. MOT has concluded formal information sharing MOUs with Belgium, Aruba and the Netherlands Antilles. The Netherlands is a party to the 1988 UN Drug Convention and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. The Dutch participate in the Basel Committee, and have endorsed the Committee's "Core Principles for Effective Banking Supervision." The Netherlands is a party to the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime.

The Netherlands should continue the strong enforcement of its anti-money laundering program and its leadership in the international arena.

### **Netherlands Antilles**

The Netherlands Antilles, which has autonomous control over its internal affairs, is a part of the Kingdom of the Netherlands. The Netherlands Antilles is comprised of Curacao, Bonaire, the Dutch part of Sint Maarten/St. Martin, Saba, and Sint Eustatius. The Government of the Netherlands Antilles (GONA) is located in Willemstad, the capital of Curacao, which is also the financial center of the five islands. Narcotics-trafficking and a lack of border control between Sint Maarten and St. Martin create opportunities for money launderers in the Netherlands Antilles. The Netherlands is reported to be the most significant source of suspicious transactions. Of note is the surge over the past few years of remittance transfers from the Netherlands.

The Netherlands Antilles has a significant offshore financial sector with 39 international banks and approximately 50 trust companies providing financial and administrative services to their international clientele, including approximately 18,750 international companies, mutual funds, and international finance companies. The laws and regulations on bank supervision state that international banks must have a physical presence on the island and hold records there. The Central Bank supervises the international banks. Authorities in other countries supervise some mutual funds. In early 2003, legislation was introduced to transfer supervision of the trust sector to the Central Bank. International corporations may be registered using bearer shares. The practice of the financial sector in the Netherlands Antilles is for either the bank or the company service providers to maintain copies of bearer share certificates for international corporations, which include information on the beneficial owner(s). There is a proposal to require that the name of the ultimate beneficial owner of the bearer share be recorded in a registry and made accessible to law enforcement officials upon a treaty-based request for the information.

The free trade zones are minimally regulated; however, administrators and businesses in the zones have indicated an interest in receiving guidance on detecting unusual transactions.

Money laundering is a crime. Legislation in 1993 and subsequent interpretations regarding the "underlying crime" establish that prosecutors do not need to prove that a suspected money launderer also committed an underlying crime in order to obtain a money laundering conviction. Thus, it is sufficient to establish that the money launderer knew, or should have known, of the money's illegal origin.



In recent years, the GONA has taken steps to strengthen its anti-money laundering regime by expanding suspicious activity reporting requirements to gem and real estate dealers; introducing indicators for the reporting of unusual transactions for the gaming industry; issuing guidelines to the banking sector on detecting and deterring money laundering; and modifying existing money laundering legislation that penalizes currency and securities transactions, by including the use of valuable goods. The 2002 "National Ordinance on the Supervision of Fiduciary Business," institutes a Supervisory Board that oversees the international financial sector. At the same time, GONA subjected the members of this sector to know-your-customer rules. A GONA interagency anti-money laundering working group cooperates with its Kingdom counterparts.

Onshore banks are increasingly using their discretionary authority to protect themselves against money laundering. The largest commercial bank lowered its limits on moneygrams to \$2,000. Banks are reluctant to do business with the Internet gaming providers, provoking complaints from that sector. In 2003 Curacao was reported to have six sports booking sites and 100 Internet casinos. The MOT NA has issued a manual for casinos on how to file reports and has started to install software in casinos that will allow reports to be submitted electronically.

In May 2002 cross-border currency reporting legislation came into force. The law specifies reporting procedures for an individual bringing in or taking out more than NAF 20,000 (approximately \$11,000) in cash or bearer instruments, and also applies to courier services. Declaration of currency exceeding the limit must include origin and destination. There is a fine of up to NAF 500,000 (approximately \$280,900) or one year in prison. In July 2003, Sint Maarten Customs seized \$11,500 from a traveler, and in August 2003, \$20,000 in undeclared currency was seized from a Curacao passenger.

Unusual transactions are by law reported to the Financial Intelligence Unit (FIU), the Netherlands Antilles Reporting Center, Meldpunt Ongebruikelijke Transacties (MOT NA). On June 1, 2003, the Central Bank issued new consolidated reporting guidelines, replacing those of 1996. These guidelines are more closely focused on banks, insurance companies, pensions funds, money transfer services, and financial administrators now specifically include counterterrorism detectors. The Central Bank also established a Financial Integrity Unit to monitor corporate governance and market behavior. Entities under supervision must submit an annual statement of compliance.

The current staff of seven at the MOT NA continues to work diligently to enhance the effectiveness and efficiency of its reporting system. Significant progress has been made in automating suspicious activity reporting; in 2002 reporting institutions sent 99.2 percent of their reports to the MOT NA electronically. All are now done on-line, and most of the matches with external databases will be done electronically. The MOT NA transmits information electronically to the police. On October 18, 2002, the GONA published new indicators for the reporting of unusual transactions with regard to terrorism financing. The new indicators require that unusual transactions reported to the police or judicial authorities in connection with money laundering or the financing of terrorism must also be reported to the MOT NA. This requirement also extends to unusual transactions relating to credit cards, money transfers and game of chance transactions.

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

In January 2002, the GONA enacted legislation allowing a judge or prosecutor to freeze assets related to the Taliban cum suis and Usama Bin Ladin cum suis (cum suis means that all companies and persons connected with the Taliban or Usama Bin Ladin are included). The legislation contains a list of individuals and organizations suspected of terrorism. The Central Bank instructed financial institutions to query their databases for information on the suspects and to immediately freeze any assets that were found. In October 2002, the Central Bank instructed the financial institutions under its supervision to continue these efforts and to consult the UN website for updates to the list.

Netherlands Antilles law allows the exchange of information between the MOT NA and foreign FIUs by means of memoranda of understanding and by treaty. The MOT NA's policy is to answer requests within 48 hours after receipt, although this timeframe is not always met. An agreement was signed in April 2002 between the Netherlands and the United States, which is also applicable to the Netherlands

Antilles, for the exchange of information with respect to taxes. This agreement was scheduled to come into force in January 2004. The Mutual Legal Assistance Treaty between the Netherlands and the United States also applies to the Netherlands Antilles. In September 2003, the U.S. Attorney in St. Thomas indicted five defendants, including one from Sint Maarten, for charges including laundering funds totaling \$68 million. Cooperation with Sint Maarten under the MLAT was an important element in the investigation.

The MOT NA is an active member of the Egmont Group. The Netherlands Antilles is a member of the Caribbean Financial Action Task Force (CFATF), and as part of the Kingdom of the Netherlands, the Netherlands Antilles participates in the FATF. In 1999, the Netherlands extended application of the 1988 UN Drug Convention to the Netherlands Antilles. The Kingdom of the Netherlands became a party to the UN International Convention for the Suppression of the Financing of Terrorism in 2002. In accordance with Netherlands Antilles law, which stipulates that all the legislation must be in place prior to ratification, the GONA is preparing legislation that will enable the Netherlands Antilles to ratify the Convention.

The Government of the Netherlands Antilles has shown a commitment to combating money laundering by establishing a solid anti-money laundering regime. An increase to the MOT NA staff is particularly notable. The Netherlands Antilles should continue its focus on increasing regulation and supervision of the offshore sector and free trade zones and pursuing money laundering investigations and prosecutions. The Netherlands Antilles should criminalize the financing of terrorists and terrorism, and should enact the necessary legislation to implement the UN International Convention for the Suppression of the Financing of Terrorism.

## **New Zealand**

New Zealand is not a major regional or offshore financial center. It has a small number of banks and financial institutions whose operations can be effectively monitored by government authorities. There is evidence that some money laundering does take place, although not to a significant extent. Narcotics proceeds and commercial crime are the primary sources of illicit funds. International organized criminal elements do operate in New Zealand.

A 1995 amendment to New Zealand's Crimes Act 1961 criminalizes laundering the proceeds of a serious offense, if the launderer knew or believed that the proceeds were derived from a serious offense. In 2003, the law was extended to apply to those who are reckless as to whether the laundered property is the proceeds of a serious offense. The Financial Transaction Reporting Act 1996 contains obligations for a wide range of financial institutions, including banks, credit unions, casinos, real estate agents, lawyers, and accountants. These entities must identify clients, maintain records, and report suspicious transactions. The Act also contains a "safe harbor" provision and requires the reporting of large cross-border currency movements.

The Terrorism Suppression Act, enacted in October 2002, criminalizes terrorist financing. This Act also made the necessary changes to the existing law to enable New Zealand to ratify the UN International Convention for the Suppression of the Financing of Terrorism. The Act gives the government wider authority to designate entities as terrorist organizations and freeze their assets. The Prime Minister is responsible for making the designation upon a recommendation prepared by the New Zealand Police. Once the designation is made, the New Zealand Police informs banks and other appropriate parties. A public notice is also published. The Police are developing additional procedures to implement the provisions of the Terrorism Suppression Act.

New Zealand has consistently implemented financial controls against entities included on the UN 1267 Sanctions Committee consolidated list. It has not yet identified in New Zealand any assets from these entities.

New Zealand and the United States do not have a Mutual Legal Assistance Treaty. However, New Zealand legislation applies certain provisions of the Mutual Assistance in Criminal Matters Act 1992 unilaterally to the United States. In practice, New Zealand and U.S. authorities have had a good record of cooperation and information sharing in this area.

New Zealand is a party to the 1988 UN Drug Convention, and in July 2002, ratified the UN Convention against Transnational Organized Crime. New Zealand is a member of the Financial Action Task Force, the Asia/Pacific Group on Money Laundering, and the Pacific Islands Forum. Its Financial Intelligence Unit is a member of the Egmont Group. The New Zealand government has played a leadership role in promoting efforts to combat money laundering in the South Pacific region, providing substantial amounts of technical assistance and training.

The Government of New Zealand has established a comprehensive anti-money laundering regime. It should build upon this base by continuing its implementation of its Terrorism Suppression Act. Additionally, New Zealand should continue its recognized leadership in the international arena.

## **Nicaragua**

Nicaragua is not a regional financial center, but continues to be a major drug transit zone. This situation makes Nicaragua's financial system an attractive target for narcotics-related money laundering. Nicaraguan officials have expressed concern that, as neighbors have tightened their money laundering laws, established Financial Intelligence Units (FIUs) and taken other actions, more illicit money has moved into the vulnerable Nicaraguan financial system. However, this concern has not resulted in much action on the part of the government. While Nicaragua has pledged to fight terrorist financing, money laundering and other financial crimes, few resources have been allocated to this effort. Nicaragua continues to exercise weak oversight and regulatory control over its financial system. Money laundering unrelated to drug-trafficking is legally undefined, and all attempts to correct this deficiency have been stalled in the National Assembly for years.

Nicaragua does not permit offshore banks to operate as such, but it does permit them to operate through nationally chartered entities (such as a Panamanian bank currently working to establish a savings and loan company under a Nicaraguan charter). Bank and company bearer shares are permitted. Nicaragua has a well-developed indigenous gaming industry, which it is only now moving to control. There are no known offshore or Internet gaming sites in Nicaragua. Nicaragua does not have any "due diligence" or "banker negligence" laws to hold bank officials responsible for their institutions' money laundering.

In 1999, Nicaragua passed Law 285 that requires banks to report cash deposits over \$10,000 to the Superintendence of Banks, which then forwards the reports for analysis to the Commission of Financial Analysis (CAF). The CAF is not a financial intelligence unit. On paper, the CAF is composed of representatives from various elements of law enforcement and banking regulators, and is responsible for detecting money laundering trends, coordinating with other agencies and reporting its findings to Nicaragua's National Anti-Drug Council. In fact, the Commission is a non-functioning entity grossly under-funded and understaffed. Even if the CAF were operational, it is unlikely that it would be effective. In Nicaragua, banks tend to close the suspicious accounts, even as they are notifying the Bank Superintendence, thereby allowing the money launderers to escape with their capital intact.

Legislation that would improve Nicaragua's anti-money laundering regime has been stalled in the National Assembly for years. Reportedly, this legislation, an amended drug law, would establish money laundering as an autonomous crime, require more stringent reporting of large and/or suspicious bank deposits, and reform and improve the CAF. It is unlikely that this reform legislation or any other major initiative in this area will make it out of the Assembly in the near or medium term.

Draft counterterrorism legislation, which would criminalize terrorist financing, is under consideration by the National Assembly, but remains far from passage. It is possible that many elements of terrorist financing can be prosecuted under existing laws. Nicaragua has the authority—through five Bank Superintendence administrative decrees—to identify, freeze, and seize terrorist-related assets, but has not, as yet, identified any such cases. Reportedly, there are no hawala or other similar alternative remittance systems operating in Nicaragua, and the Nicaraguans have not detected any use of gold, precious metals, or charitable organizations to disguise such transactions.

Nicaragua is currently negotiating a financial information sharing agreement with Costa Rica, largely based on model legislation produced by the Central American Parliament. It does not have such an agreement with the United States, but it cooperated, on an ad hoc basis, in a number of cases in

2004. This cooperation has enabled Nicaragua to benefit from several U.S. asset seizure cases and to recover \$2.7 million stolen by the former Nicaraguan tax director, and used to purchase properties in Florida. Under Law 285, 20 percent of the proceeds from drug-related asset seizures go to each of the following institutions: the Ministry of Health, the National Drug Directorate, the National Police narcotics section, the penitentiary system, and non-governmental organization drug prevention programs.

Nicaragua is a party to the 1988 UN Drug Convention. The country has also ratified the UN Convention on the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. Nicaragua is a member of the Organization of American States and the Caribbean Financial Action Task Force.

The Government of Nicaragua should expand the predicate crimes for money laundering beyond narcotics-trafficking and should criminalize terrorist financing. It should also make it a priority to allocate the resources needed to develop a fully functioning financial intelligence unit and to fully implement its anti-money laundering regime. Nicaragua should take steps to immobilize its bearer shares and adequately regulate its gambling industry. These steps would significantly strengthen the country's financial system against money laundering and terrorist financing, and would ensure compliance with relevant international standards regarding anti-money laundering controls.

## **Niger**

Niger is not a regional financial center. While there are criminal activities that take place within the region, there is no evidence to suggest that money laundering activities take place on a large scale within Niger. Seven small commercial banks and one modest-sized local bank operate in Niger. Black market currency exchanges operate freely, and currency easily flows unregulated through Niger's porous borders. Most economic activity takes place in the informal sector.

The Central Bank of West African States (BCEAO), based in Dakar, Senegal, is the Central Bank for the countries in the West African Economic and Monetary Union (WAEMU): Benin, Burkina Faso, Guinea-Bissau, Cote d'Ivoire, Mali, Niger, Senegal, and Togo, all of which use the French-backed CFA franc currency. All bank deposits over approximately \$7,700 made in BCEAO member countries must be reported to the BCEAO, along with customer identification information. In addition, all foreign currency exchanges over 1 million CFA (approximately \$1,900) require written authorization from the Niger Ministry of Finance.

In September 2002, the WAEMU Council of Ministers, which oversees the BCEAO, issued a directive requesting that each member country set up a national committee under their Minister of Finance to deal with financial information as it relates to money laundering. The BCEAO would be in charge of coordinating such committees. Each member country is now responsible for putting legislation in place to implement this directive, and the legislation is expected to be harmonized regionally. On November 27, 2003, the Niger Council of Ministers adopted a bill that formally prohibits money laundering and puts into place structures and regulations to deter such activity. The

bill became law in June 2004 after passage by the National Assembly. When in force, this law will bring Niger into conformity with the rest of the WAEMU nations. The bill called for the creation of a central office at the BCEAO for the coordination of money laundering issues and formally obliges all financial institutions in Niger to report suspicious activity. The office was established in 2004. Currently, banks in Niger report suspicious activity to the BCEAO and to local law enforcement, although there are no legal requirements to do so. In 2002, one bank account in Niger was frozen due to its relationship to illegal financial activity.

The WAEMU Council of Ministers also issued a directive in September 2002 on the topic of terrorist financing, requesting member countries to pass legislation requiring banks to freeze the accounts of any persons or organizations on the UN 1267 Sanctions Committee's consolidated list. In addition, the Government of Niger (GON) and the BCEAO actively comply with U.S efforts to combat terrorist financing. When notified of persons or entities designated by the UN 1267 Sanctions Committee's consolidated list or the list of Specially Designated Global Terrorists designated by the U.S. pursuant to E.O 13224, the BCEAO promptly disseminates information to all financial institutions in Niger. Since

January 1, 2004, there have been no reported cases of money laundering or terrorist financing in Niger.

In 2000, the Economic Community of West African States (ECOWAS) established the Intergovernmental Group for Action Against Money Laundering (GIABA), based in Dakar, Senegal. In November 2002, GIABA hosted an anti-money laundering seminar for representatives of 14 ECOWAS members, including Niger. In July 2002, Niger participated in the 2002 West African Joint Operation Conference (WAJO) that promotes regional law enforcement cooperation against drug trafficking, terrorism, and money laundering. In April 2004, The National Assembly adopted a domestic law on money laundering to implement GIABA. In September 2004, Niger ratified the UN Convention against Transnational Organized Crime and acceded to the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Niger should continue to implement all the provisions of the 2004 anti-money laundering laws.

## **Nigeria**

The Federal Republic of Nigeria is the most populous country in Africa and is West Africa's largest democracy. Nigeria's large economy is also a hub of trafficking of persons and narcotics. Nigeria is a major drug-transit country. Nigeria is a center of criminal financial activity for the entire continent. Individuals and criminal organizations have taken advantage of the country's location, weak laws, systemic corruption, lack of enforcement, and poor economic conditions to strengthen their ability to perpetrate all manner of financial crimes at home and abroad. Nigerian criminal organizations have proven adept at devising new ways of subverting international and domestic law enforcement efforts and evading detection. Their success in avoiding detection and prosecution has led to an increase in many types of financial crimes, including bank fraud, real estate fraud, identity theft, and advance fee fraud. Despite years of government effort to counter rampant crime and corruption, Nigerians continue to be plagued by crime. The Government of Nigeria (GON) has made efforts to counteract these crimes but, despite some successes in 2004, socio-economic conditions have impeded its efforts.

In addition to narcotics-related money laundering, advance fee fraud is a lucrative financial crime that generates hundreds of millions of illicit dollars annually for criminals. Initially, Nigerian criminals made advance fee fraud infamous; more recently, nationals of many African countries and from a variety of countries around the world have begun to perpetrate advance fee fraud. This type of fraud is referred to internationally as "Four-One-Nine" fraud (419 is a reference to the fraud section in Nigeria's criminal code). While there are many variations, the main goal of 419 fraud is to deceive victims into payment of an advance fee by persuading them that they will receive a very large benefit in return. These "get rich quick" schemes have ended for some victims in monetary losses, kidnapping, or murder. Through the Internet, businesses and individuals around the world have been and continue to be targeted by perpetrators of 419 scams.

In June 2001, the Financial Action Task Force (FATF) placed Nigeria on its list of noncooperative countries and territories (NCCT) in combating money laundering. Among the deficiencies cited by the FATF were the failure to criminalize money laundering for offenses other than those related to narcotics, the lack of customer identification requirements for over-the-counter transactions under a threshold of \$100,000, inadequate suspicious transaction reporting requirements, the absence of anti-money laundering measures applied to stock brokerage firms and other financial institutions, and a high level of government corruption. In April 2002, FinCEN, the U.S. financial intelligence unit, issued an advisory to inform banks and other financial institutions operating in the United States of serious deficiencies in the anti-money laundering regime of Nigeria.

In June 2002, the FATF stated that it would consider recommending countermeasures against Nigeria at its October 2002 plenary if Nigeria did not engage with the FATF Africa Middle East Review Group and move quickly to enact legislative reforms that addressed FATF concerns. In October 2002, the FATF recommended countermeasures against Nigeria if the Government of Nigeria (GON) did not enact sufficient legislative reforms by December 15, 2002. That same month, Nigeria submitted an anti-money laundering implementation plan to the FATF, but it was deemed insufficient to justify delisting Nigeria.

On December 14, 2002, the National Assembly of Nigeria passed three pieces of anti-money laundering legislation, and President Olusegun Obasanjo signed the legislation into law the same day: an amendment to the 1995 Money Laundering Act that extends the scope of the law to cover the proceeds of all crimes; an amendment to the 1991 Banking and Other Financial Institutions (BOFI) Act that expands coverage of the law to stock brokerage firms and foreign currency exchange facilities, gives the Central Bank of Nigeria (CBN) greater power to deny bank licenses and allows the CBN to freeze suspicious accounts; and the Economic and Financial Crimes Commission (Establishment) Act that establishes the Economic and Financial Crimes Commission (EFCC), that coordinates anti-money laundering investigations and information sharing. The Economic and Financial Crimes Commission Act (2002) also criminalizes the financing of terrorism and participation in terrorism. Violation of the Act carries a penalty of up to life imprisonment. Based on this legislation, FATF decided not to recommend countermeasures against Nigeria; however, Nigeria remains on the NCCT list.

In April 2003, the EFCC was formally constituted, with the primary mandate to investigate and prosecute financial crimes. It has recovered or seized assets from various people guilty of fraud inside and outside of Nigeria, including a syndicate that included highly placed government officials who were defrauding the Federal Inland Revenue Service (FIRS). Several influential individuals have been arrested and are currently awaiting trial. In an effort to expedite the trial process, the Commission has been assigned two high court judges in Lagos and two in Abuja to hear all cases involving financial crimes. This signals intent by the government to more aggressively investigate "419" and other economic crimes in Nigeria.

In 2004, the National Assembly passed the Money Laundering (Prohibition) Act (2004), which applies to the proceeds of all financial crimes. It also covers stock brokerage firms and foreign currency exchange facilities, in addition to banks and financial institutions. The legislation gives the CBN greater power to deny banks licenses and freeze suspicious accounts. This legislation strengthens the financial institutions by also requiring more stringent identification of accounts, removing a threshold for suspicious transactions, and lengthening the period for retention of records.

However, in November 2004, the Chairman of the EFCC stated publicly that over 90 percent of Nigeria's banks were not in compliance with the new law. He said that banks were not adhering to the know-your-customer and know-your-customer's-business provisions of the law, and that 95 percent of banks had not yet filed any suspicious transactions reports (STRs), something he deemed "suspicious by itself." However, he vowed to promulgate a new initiative to educate bank personnel and the general public about the provisions of the law before he began imposing sanctions for non-compliance.

The EFCC recorded some successes in 2004 in the area of combating money laundering, including the arrest of several notorious advance fee fraud kingpins, who are currently being prosecuted. These include a group involved in the Brazilian bank scam that totaled \$242 million. The EFCC seized assets worth about \$300 million in 2004. The EFCC was involved in the prosecution of more than 100 high-profile financial crime cases in the Nigerian High Court, including bank fraud, tax evasion, and money laundering. For the first time in the history of the country, a sitting provincial governor is being tried for corruption and money laundering, and several other money laundering cases are being tried. There was one money laundering conviction in 2004. The EFCC established a Financial Intelligence Unit (FIU) in 2004 that is now receiving and analyzing STRs. However, as noted above, very few such reports have yet been filed.

Nigeria is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. On December 9, 2003, Nigeria signed the UN Convention against Corruption. The United States and Nigeria have a Mutual Legal Assistance Treaty, which entered into force in January 2003. Nigeria has signed memoranda of understanding with Russia, Iran, India, Pakistan, and Uganda to facilitate cooperation in the fight against narcotics-trafficking and money laundering. Nigeria has also signed bilateral agreements for exchange of information on money laundering with South Africa, the United Kingdom, and all Commonwealth and Economic Community of West African States countries. Nigeria has been instrumental in the establishment of a permanent secretariat for the Intergovernmental Task Force Against Money Laundering in West Africa (GIABA).

The Government of Nigeria should continue to engage with the FATF to ensure that Nigeria's remaining anti-money laundering deficiencies are corrected. It should also bolster the Economic and Financial Crimes Commission by ensuring that it is adequately funded. Nigeria should construct a comprehensive anti-money laundering regime that willingly shares information with foreign regulatory and law enforcement agencies, is capable of thwarting money laundering and terrorist financing, and comports with all relevant international standards. Nigeria should criminalize the financing of terrorism consistent with the UN International Convention for the Suppression of the Financing of Terrorism.

## **Niue**

Niue is a self-governing parliamentary democracy in the South Pacific that maintains a free association with New Zealand. Niueans are citizens of New Zealand and are part of the British Commonwealth.

Concerns were raised in the past about Niue's vulnerability to money laundering. Legislation from the mid-1990s created an offshore financial center heavily dependent upon international business companies (IBCs). In addition, a small number of offshore banks were licensed. Niue also offers trusts, partnerships, financial management, and insurance services. Niue allows the creation of asset protection trusts that are impervious to many types of legal claims arising in other jurisdictions. In addition, trusts in Niue are exempt from taxation if the parties to the trust are not residents of Niue.

The International Business Companies Act of 1994 is the legislative basis for establishing international business companies. Marketers of offshore services promote Niue as a favored jurisdiction for establishing IBCs, for a variety of reasons. The presence of a significant number of international business companies operating offshore makes Niue particularly vulnerable to money laundering. With a population of roughly 2,100, Niue reported that it had registered 9,229 IBCs as of December 2003. Allowed under Niue's International Business Companies Act 1994, the IBCs are not required to disclose their beneficial ownership or to keep a register of directors. Moreover, Niue allows bearer shares and the marketing of shelf companies, which are offered by Internet marketers complete with associated offshore bank accounts and mail-drop forwarding services. The IBCs are legally formed and registered by a Panamanian law firm on Niue's behalf. The government reported in December 2003 that it had not registered any offshore financial service businesses, such as insurance companies, mutual fund companies, trust companies, and agents.

The Proceeds of Crime Act 1998 criminalizes the laundering of proceeds from any offense punishable by at least one year in prison. Under the Proceeds of Crime Act, financial institutions may report suspicious transactions either to the police or to the Attorney General. However, there have been no such reports, and there are no relevant procedures in place to deal with their possible collection and analysis. Currently, the Proceeds of Crime Act allows the court to order the confiscation or forfeiture of property derived from a serious offense, once the offender has been convicted. The Act does not specifically address assets derived from narcotics-trafficking, terrorism financing, or organized crime. The government is working to amend the Act to allow it to freeze transactions in which money laundering or terrorism financing is suspected.

Niue enacted the Financial Transactions Reporting Act (FTRA) in November 2000. The FTRA imposes reporting and record keeping obligations upon banks, insurance companies, securities dealers and futures brokers, money services businesses, and persons administering or managing funds on behalf of IBCs. Specifically, the FTRA requires financial institutions to report suspicious transactions, verify the identity of their customers, and keep records of financial transactions for six years. However, the act contains a number of loopholes that result in inadequate customer identification requirements, among other deficiencies. For example, Section 11 of the FTRA requires that financial institutions verify the identity of customers who wish to conduct a transaction. Subsection 11(2) provides a loophole in that a financial institution dealing with an intermediary need establish the identity of the underlying customer only if the transaction exceeds \$10,000.

The FTRA also calls for the establishment of a Financial Intelligence Unit (FIU) within the office of the Attorney General. The FIU has still not been established. Niuean officials have said that the establishment of the FIU will depend upon the outcome of ongoing discussions among the Pacific

Islands Forum of a proposed regional FIU for Forum member countries. To date, no movement has been made towards the establishment of any operational FIU, domestic or regional.

Should a Niuean FIU become operational, financial institutions will be required to prepare a written statement of their internal procedures to make their officers and employees aware of the laws in Niue about money laundering; the procedures, policies, and audit systems adopted by the institution to deal with money laundering; and procedures to train the institution's officers and employees to recognize and deal with money laundering. The institutions then will have to submit the statement of those procedures to the FIU. The FIU will also have powers to conduct investigations to ensure compliance by financial institutions with the Financial Transactions Reporting Act 2000. Currently, casinos and notaries are not covered within the definition of "financial institution" under the Act, but the government is considering promoting an amendment that would substitute the definition of "financial institution" from the IMF model Financial Transactions Reporting Act.

The Financial Transactions Reporting Act 2000 provides that one of the functions of the financial intelligence unit is to issue guidelines to financial institutions in relation to transaction record keeping and reporting obligations and to provide training programs for financial institutions about transaction record keeping and reporting obligations.

In June 2002, Niue brought into force the International Banking Repeal Act. This Act eliminated Niue's offshore banks. As a result, all offshore banking licenses have been terminated. In addition, Niue now maintains in-country a mirror of the IBC registry kept in Panama. All company registration information is kept on the island by a registered agent and is accessible to appropriate officials.

Due to these reforms, the Financial Action Task Force (FATF) decided in October 2002 that Niue had in place an anti-money laundering system that generally meets international standards. Niue was therefore removed from the list of Non-Cooperative Countries or Territories (NCCT), on which it had been placed in June 2000. With Niue's removal from the NCCT list, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) lifted its advisory that had instructed all U.S. financial institutions to "give enhanced scrutiny" to all transactions involving Niue.

Niue is not a member of the United Nations. In November 2001, the government amended the United Nations Act 1946 to enable the Cabinet to promulgate regulations giving effect to UN Security Council resolutions. And, in September 2003, the Cabinet passed the United Nations Sanctions (Terrorism Suppression and Afghanistan Measures) Regulations 2003. Those regulations implement UN Security Council Resolution 1373, as well as Resolutions 1267 and 1333.

Niue is a member of the Asia/Pacific Group on Money Laundering.

In 1998, Niue passed the Mutual Assistance in Criminal Matters Act, which authorizes the Attorney General of Niue to provide certain types of legal assistance to other countries involved with criminal investigations. Niue has no bilateral cooperation agreements with other countries for the exchange of information on money laundering, though the government has expressed a willingness to cooperate with international efforts to combat money laundering.

The Government of Niue's recent reforms address some of the deficiencies in Niue's anti-money laundering regime; however, the government must finalize and promulgate the necessary regulations to bring the legislation into full force, including the establishment of a Financial Intelligence Unit (FIU). Niue must ensure that the recently enacted reforms are fully and effectively implemented. Additionally, Niue should criminalize terrorist financing.

## **Norway**

Norway is not considered an important regional financial center. However, criminal activity, particularly connected with narcotics and economic crime, is increasing in Norway. According to Oekokrim, the economic crime unit of the Ministry of Justice, which serves as Norway's Financial Intelligence Unit (FIU), the rise in crime has been marked by increases in specialization, cooperation between criminal networks, links between criminal and legal business activities, and the use of advanced technologies.



Violent and professional armed robberies, often by foreigners, have also become more frequent. Authorities suspect that the proceeds of the robberies are laundered through registered companies formally or informally controlled by the criminals. Most money laundering occurs outside the banking and financial services system of Norway, due to the reporting requirements of the financial institutions; however, structuring of deposits still appears to be a problem within the financial system. Norway does not have a significant market for smuggled goods. Norway has neither free trade zones nor an offshore banking system.

In accordance with the Norwegian Penal Code, all forms of money laundering are criminal offenses. Norway's anti-money laundering legislation has been strengthened in recent years to conform to the Financial Action Task Force (FATF) Forty Recommendations. In 2004, a new Money Laundering Law took effect, replacing the provisions of the 1988 Financial Institutions Act. The new act strengthens registration requirements, broadens the obligation to report suspicious transactions, and makes negligent contravention of the act a criminal offense.

The Banking, Insurance, and Securities Commission of Norway monitors the financial markets and financial institutions, issues warnings, forwards the consolidated UNSCR 1267/1390 list of terrorist entities and individuals to financial institutions, and issues orders to freeze assets and funds. The Commission conducts on-site inspections to monitor the finance sector and to ensure that the regulations are complied with correctly. The Commission has also taken steps to strengthen reporting requirements of charitable entities.

All financial institutions are required to report large and suspicious transactions to Oekokrim, verify the identity of their customers, and keep records of transactions for at least five years. Money laundering controls are also applied to all non-bank financial institutions, such as insurance companies. Financial institutions are required to report large cash transactions, including cross-border transactions, to the Norwegian Central Bank, specifying sender and recipient information. Norway has not enacted secrecy laws that prevent disclosure of client and ownership information to bank supervisors and law-enforcement authorities. Individual bankers may be held responsible if their institutions launder money; however, the law protects reporting individuals. The number of money laundering infractions reported by traditional financial institutions decreased during the first half of 2004. Oekokrim's money laundering unit attributes the decline to the financial institutions' initial uncertainty regarding procedures under the new Money Laundering Act and to their decision to focus on the most serious and complex cases.

Through June 30, 2004, Norwegian authorities initiated 292 money laundering investigations. A total of 245 cases resulted in indictments or fines, and there were 100 court convictions for money laundering. Most money laundering cases in Norway are related to domestic criminal activity, and no terrorist groups are known to have laundered funds in the country.

According to Norwegian laws, assets derived from criminal acts (narcotics-trafficking, money laundering, and support for terrorism), are to be seized and confiscated by the State. Oekokrim continues to establish systems for identifying, tracing, freezing, seizing, and forfeiting narcotics-related assets and remains the principal entity responsible for tracing and seizing assets, although any police unit may do so in Norway. Section 34 of the Penal Code establishes that confiscation is mandatory unless a court finds that the confiscation is unreasonable. In serious cases, the law allows for extended confiscation. The offender must be found guilty of a criminal act from which considerable proceeds are accrued. Considerable proceeds are defined as at least NOK 75,000 (\$12,000). Legitimate businesses may be seized if they are used to launder drug money or support terrorist activity, or are linked to other criminal proceeds. Substitute assets may be seized. Norway destroys seized drugs, alcohol, and cigarettes, but auctions off other items, including automobiles, private property, and buildings. The State receives the proceeds from the asset seizures and forfeitures. The law allows civil as well as criminal forfeiture. In 2003 authorities issued 929 confiscation orders totaling over \$24 million. To date, Norway has not enacted laws for sharing narcotics assets with other countries.

On June 28, 2002, Norway enacted Section 147 (A-B) of the Penal Code, criminalizing the financing of terrorism. The new bill establishes legislative measures against acts of terrorism and the financing of terrorism, which fulfill the requirements of the UN International Convention for the Suppression of the

Financing of Terrorism. The law applies to anyone who supplies funds to, or collects funds for, individuals or groups that plan acts of terrorism, and makes the support of terrorists with equipment or services a criminal offense. Norway has the authority to identify, freeze, and seize terrorist financial assets. There were no arrests or prosecutions for terrorist financing, and Oekokrim did not receive any suspicious transaction reports related to terrorism in 2004. Authorities have investigated one suspected instance of terrorist financing, but the case was dropped in 2004.

On October 11, 2002, Norway adopted the European Union's (EU's) Common Position on the application of specific measures to combat terrorism. The Common Position details the names of major terrorists groups. Norway has also distributed to financial institutions the UNSCR 1267 Sanctions Committee's consolidated list. In accordance with UNSCR 1267, the bank account of one individual has been frozen since February 2003. The amount frozen was approximately \$1,000.

Alternative remittance systems are prohibited in Norway. In November 2004, a Norwegian appellate court upheld the convictions of three Somalis accused of violating banking regulations by sending unauthorized remittances overseas. The prosecutor in the case reported that the men illegally remitted approximately \$6 million annually between 1998 and 2001. The ringleader of the scheme was sentenced to a one-year jail sentence and his two accomplices were fined approximately \$1,500 each.

Norway works with Europol and is a member of the FATF, Interpol, and Schengen. Oekokrim is a member of the Egmont Group. Norway is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Corruption. Norway is also a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime; the UN International Convention for the Suppression of the Financing of Terrorism; and the UN Convention against Transnational Organized Crime. Norway has now ratified all 12 of the International Conventions and Protocols relating to terrorism. Norway consults frequently with United States authorities in connection with investigations and proceedings related to narcotics, terrorism, terrorist financing, and other crimes. Norway's Money Laundering Act and Terrorist Financing Law ensure the availability of adequate records in connection with investigations of interest to the United States and other governments.

The Government of Norway should continue to enhance its anti-money laundering/counterterrorist financing regime. Norway should consider the adoption of laws that would allow the sharing of seized assets with third party jurisdictions that assisted in the conduct of the underlying investigation.

## **Oman**

Oman is not a regional or offshore financial center and does not have a significant money laundering problem. Its small banking sector is supervised by the Central Bank of Oman (CBO), which has the authority to suspend or reorganize a bank's operations. In 2004, Oman had a total of 17 banks with 353 branches. The banking system consisted of five local commercial banks with 304 Omani and 11 foreign branches, three local specialized banks with 26 local branches, and nine foreign incorporated banks with 23 branches in the country. Smuggling trade goods across Oman's long borders and coastline is becoming an increasing concern. Oman may also be vulnerable to instances of trade-based money laundering and customs fraud as well as unregulated lending schemes that fall outside government purview.

In March 2002, Royal Decree No. 34/2002 was issued promulgating "The Law of Money Laundering." This new law strengthened the existing money laundering regulations by detailing bank responsibilities, widening the definition of money laundering to include funds obtained through any criminal means, and providing for the seizure of assets and other penalties. The new law applies to other types of non-bank financial institutions, as well. In a 2003 report to the UN Counter-Terrorism Committee, Omani officials stated that "the legal freezing measures designated by the Money laundering Act are applied to both residents and non-residents holding funds, financial assets, or other economic resources in the Sultanate of Oman if they are linked to terrorist-related activities." In addition to an interagency committee for Anti-Money Laundering, the Sultanate has established a senior-level National Committee for Combating Terrorist Finance.

Royal Decree 72/2004 of July 7, 2004 promulgated the implementing regulations for the Law of Money Laundering. These regulations include, inter alia, the following provisions: a requirement that financial

institutions "take steps to obtain information on customers who open accounts in an indirect way" and "keep electronic data on e-transactions"; guidelines in the area of profiling, requiring institutions to "check and double-check" certain classes of transactions (e.g., "customers getting loans from foreign institutions" and the "keeping of accounts that do not match the business nature"); requirements for government authorities to investigate all "suspicious dealings" using internal and external reporting mechanisms; authorization for the attorney general to freeze disputed assets upon the request of investigators; protection of "secret" information; an extensive training program, with introductory courses supplemented by instruction in international best practices and effective investigation techniques; definition of the organizational structure of the National Committee for Combating Money Laundering; and, cooperation with international organizations and information exchange with other countries, including collaboration on extradition issues.

The Royal Oman Police (ROP), in coordination with the CBO, is responsible for investigating money laundering activities. Banks are required to know their customers and report all suspicious transactions. Compliance personnel are now present in all banks. Oman plans to establish a Financial Intelligence Unit (FIU) that will review suspicious transactions and help coordinate resulting investigations. As of the end of 2004, there had been no arrests under the new law. No formal mechanism currently exists for information sharing among the Central Banks or FIUs of the Gulf Cooperation Council (GCC) members, although a banking supervision committee within the GCC does issue broad guidelines for financial institution oversight.

Oman regulates charitable organizations under the Non-Governmental Organizations Act promulgated pursuant to Royal Decree 14/2000. Under this act, the Minister of Social Development is responsible for approving and monitoring all charitable contributions and fundraising activities. There is a government-registered charity (the Oman Charitable Organization, or OCO), and all citizens and entities are encouraged to use this official channel for donations. The Ministry of Social Development recently registered a charity fund run by a prominent local businessman. At various times, charitable donations have been collected through individual accounts in local banks and sent abroad by individuals to support different causes, such as the Palestinian Intifada and the building of schools or mosques in Africa and South Asia. The local Shia minority is believed to transfer money to support their religious imams, mainly in Iraq and Iran. Apart from monthly remittances by expatriate laborers, local Indian businessmen have also been reported to channel funds in support of Hindu religious groups. In all of these cases, the CBO possesses the authority and ability to check on these accounts, as all banks and moneychangers have the obligation to report on transactions.

Informal lending societies reportedly have emerged in recent years as a popular alternative to formal banking in Oman. These societies provide interest free loans as a means for young Omanis to purchase homes and cars or service bank debts. The societies became the target of three separate warnings from the Ministry of Social Development calling on Omanis to avoid these unregulated and unregistered financial entities. Nevertheless, many Omanis flocked to these societies in solidarity with members of their tribes and in protest against double-digit interest rates being charged by commercial banks. Later, as membership numbered in the thousands, serious problems emerged as several founding members absconded with funds from their societies. Suspicious members withdrew from the schemes, causing the collapse of many societies. Transactions in these societies are made in cash, and the societies are not registered with any government agency or institution. While such practices constitute only a fraction of overall financial transactions in Oman, they merit greater scrutiny on the part of ROP and CBO authorities. Reports of excess liquidity in the Omani financial system and the demonstrated popularity of informal societies lend credence to the view that a significant amount of wealth, amounting to hundreds of thousands if not millions of dollars, is circulating outside the formal financial system and its strict regulations, auditing requirements, and accountability to the CBO.

Oman has responded to terrorist asset freeze lists from the UN 1267 Sanctions Committee by distributing the lists to all banks and other financial institutions in the country for checking against their accounts. Thus far, the Government has reported negative results. Oman is a party to the 1988 UN Drug Convention. Although not yet a party to the UN International Convention for the Suppression of the Financing of Terrorism, Omani officials insist that Oman will soon accede. Oman has yet to sign the UN Convention against Transnational Organized Crime. Oman is a member of the Gulf Cooperation Council (GCC), which itself is a member of the Financial Action Task Force (FATF). Oman is also a charter member of the Middle East and North Africa Financial Action Task Force (MENAFATF) that was inaugurated in Bahrain in November 2004. The MENAFATF is a FATF-style

regional body. The creation of the MENAFATF is critical for pushing the region to improve the transparency and regulatory frameworks of its financial sectors. Overall, the Government of Oman maintains a strong and effective regulatory regime with respect to its formal financial institutions. Oman should continue to implement its anti-money laundering program, specifically by establishing and dedicating adequate resources to its Financial Intelligence Unit (FIU) and training criminal investigators to initiate money laundering investigations from the field. Oman also should address the risks of alternative remittance systems and unregulated lending societies to launder money and sidestep formal government oversight of financial transactions. Applying the careful lessons learned in its tight regulation of the formal sector, Oman must now recognize that informal money transfer and cash-based lending societies represent vulnerabilities that must be addressed. Oman should sign and ratify both the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime.

## **Pakistan**

Financial crimes related to narcotics-trafficking, terrorism, smuggling, tax evasion, and corruption remain a significant problem in Pakistan. Pakistani criminal networks play a central role in the transshipment of narcotics and smuggled goods from Afghanistan to international markets. Pakistan is a major drug-transit country. The proceeds of narcotics-trafficking and funding for terrorist activities are often laundered by means of the alternative remittance system called hawala. This system is also widely used by the Pakistani people for legitimate purposes. A network of private unregulated charities has also emerged as a major source of illicit funds for international terrorist networks.

Pakistan's current anti-money laundering regime is weak, outdated and based on a loose patchwork of laws and regulations. The major laws include: The Anti-Terrorism Act of 1997 (amended in October 2004 to increase maximum punishments), which defines the crimes of terrorist finance and money laundering and establishes jurisdictions and punishments; The National Accountability Ordinance of 1999, which requires financial institutions to report suspicious transactions to the National Accountability Bureau (NAB) and establishes accountability courts; and The Control of Narcotic Substances Act of 1997, which also requires the reporting of suspicious transactions, contains provisions for the freezing and seizing of assets associated with narcotics-trafficking, and establishes special courts for offenses (including financing) involving illegal narcotics. The State Bank of Pakistan (SBP) and the Securities and Exchange Commission of Pakistan (SECP) regulate financial flows.

Since 2002, Pakistan's Ministry of Finance has been coordinating an interministerial effort to draft anti-money laundering and counterterrorist financing legislation, with the goal of bringing Pakistan into compliance with international norms. As of December 2004, this legislation had not received final cabinet approval, and therefore, had not been submitted to the National Assembly for enactment. The latest version of that legislation was reviewed by a delegation from a FATF-style regional body, the Asia/Pacific Group on Money Laundering (APG), in December 2004. The draft law, among other things, provides for a Financial Intelligence Unit (FIU), which does not currently exist in Pakistan.

Notwithstanding the absence of such legislation, the SBP, which serves as Pakistan's Central Bank, has created an anti-money laundering unit. It has also introduced FATF-compliant regulations in the areas of know-your-customer policy, record retention, due diligence of correspondent banks, and the reporting of suspicious transactions. The SECP, which has regulatory oversight for non-bank financial institutions, has applied know your customer regulations to stock exchanges, trusts, and other non-bank financial institutions. All transactions exceeding RS 50,000 (approximately \$847) must be carried out via check or bank draft, as opposed to cash. The NAB, the Anti-Narcotics Force, the Federal Investigative Agency, and the Customs authority oversee Pakistan's anti-money laundering efforts. The National Accountability Bureau has been effective in investigating and prosecuting corruption, but has been accused of political bias in selecting its targets.

Pakistan's cooperation in Operation Enduring Freedom has brought renewed focus on the role of informal financial networks in financing terrorist activity. In June 2004, the SBP required all hawalas to register as authorized foreign exchange dealers and to meet minimum capital requirements. Failure to comply was punished by forced closures. However, despite increased enforcement efforts, unregistered hawalas continue to operate illegally. A large percentage of hawala transfers to Pakistan consists of the repatriation of wages from the roughly five million Pakistani expatriates residing abroad.

Nevertheless, the U.S. Government has observed a migration of an increasing number of transactions from the informal to the formal financial institutions sector, due to the GOP's regulation of the domestic hawala business, post-September 11 changes in the patterns of behavior of overseas Pakistanis, and a substantial increase in credit available in the formal financial sector.

There have been reports of money laundering in Pakistan using gold and gems, as well as cash transfers by couriers. Pakistani criminal networks play a central role in the transshipment of narcotics and smuggled goods from Afghanistan to international markets. Trade-based money laundering is also prevalent. Goods such as foodstuffs, electronics, vegetable oils, and other products that are primarily exported from Dubai to Karachi are then forwarded, at least on paper, to Afghanistan via the Afghan transit trade. Through smuggling, corruption, avoidance of customs duties and taxes, and barter deals for narcotics, many of the goods destined for Afghanistan find their way into the burgeoning Pakistani black market. The trading in these goods and commodities is also believed to be used to provide counter valuation in hawala transactions. A nexus of private, unregulated charities has also emerged as a major source of illicit funds for international terrorist networks. As of December 28, 2004, Pakistan's Central Bank had frozen roughly \$10.5 million belonging to 12 entities and individuals, in compliance with UNSCR 1267.

Pakistan is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. As of December 2004, Pakistan had not signed the UN International Convention for the Suppression of the Financing of Terrorism. Pakistan became a member of the APG in 2000.

The Government of Pakistan should move quickly to enact anti-money laundering and counterterrorist financing legislation that conforms to international standards. It also should issue financial regulations that mandate the reporting of all suspicious transactions, and establish a Financial Intelligence Unit. In addition, in light of the role that private charities have played in terrorist financing, Pakistan should develop a system to regulate the finances of charitable organizations and to shut down those that finance violence and terrorism. Pakistan should ratify both the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of Terrorist Financing. Greater efforts are also needed to track and suppress trade-facilitated money laundering.

## **Palau**

Palau is an archipelago of more than 300 islands in the Western Pacific with a population of nearly 20,000 and per capita GDP of about \$6,000. Upon its independence in 1994, the Republic of Palau entered the Compact of Free Association with the United States. The U.S. dollar is legal tender. Palau is not a major financial center. Nor does it offer offshore financial services. There are no offshore banks, trust companies, securities brokers/dealers or casinos in Palau. Palauan authorities believe that drug trafficking and prostitution are the primary sources of illegal proceeds that are laundered. Palau recently prosecuted its first ever case under the Money Laundering and Proceeds of Crimes Act (MLPCA) of 2001 (MLPCA) against a foreign national engaged in a large prostitution operation. The defendant was convicted on all three counts as well as a variety of other counts.

Amid reports in late 1999 and early 2000 that offshore banks in Palau had carried out large-scale money laundering activities, a few international banks banned financial transactions with Palau. In response, Palau established a Banking Law Review Task Force that recommended financial control legislation to the Olbil Era Kelulau (OEK), the national bicameral legislature, in 2001. Following that, Palau took several steps toward addressing financial security through banking regulation and supervision and putting in place a legal framework for an anti-money laundering regime. Several pieces of legislation were enacted in June 2001.

The Money Laundering and Proceeds of Crimes Act (MLPCA) of 2001 criminalized money laundering and created a financial intelligence unit. This legislation imposes threshold and suspicious transactions reporting and record keeping requirements for five years from the date of the transaction. Credit and financial institutions are required to keep regular reports of all transactions made in cash or bearer securities in excess of \$10,000 or its equivalent in foreign cash or bearer securities. This threshold reporting also covers domestic or international transfers of funds of currency or securities involving a

sum greater than \$10,000. All such transactions (domestic and/or international) are required to go through a credit or financial institution licensed under the laws of the Republic of Palau.

The Financial Institutions Act of 2001 established the Financial Institutions Commission, an independent regulatory agency, which is responsible for licensing, supervising and regulating financial institutions, defined as banks and security brokers and dealers in Palau. Currently, there are seven fully licensed banks in Palau and one with a conditional license. Six of the banks are majority foreign owned, and one is wholly Palauan owned. Three other banks had their licenses invalidated in 2002 and a license of another bank was revoked in 2003. One bank had its license revoked in early 2005 and one bank that is operating on a conditional license has met the conditions for reopening and is now functioning under the supervision of the FIC. Other entities subject to the provisions of the MLPCA, such as the seven money services businesses, two finance companies and five insurance companies, are essentially unsupervised. Once the amendments to the MLPCA are passed, all alternative money remittance systems will be licensed and regulated by the FIC. Credit and financial institutions are required to verify customers' identity and address. In addition, these institutions are required to check for information by "any legal and reasonable means" to obtain the true identity of the principal/party upon whose behalf the customer is acting. If identification cannot, in fact, be obtained, all transactions must cease immediately.

The lack of both human and fiscal resources has hampered the development of a viable anti-money laundering regime in Palau. The Republic has only recently established a functioning Financial Intelligence Unit (FIU), though its operations are severely restricted by a lack of dedicated human and fiscal resources. The implementing regulations to ensure compliance with the MLPCA have yet to be written but the authorities have stated that they will be drafted once the revisions to the MLPCA have been passed. The will of the Executive branch to comply with international standards, however, was clearly demonstrated by President Remengesau in 2003, when he vetoed a bill that would have extended the deadline for bank compliance and would have reduced the minimum capital for a bank from \$500,000 to \$250,000. Additionally, the President established the Anti-Money Laundering Working Group that is comprised of the Office of the President, the FIC, the Office of the Attorney General, Customs, the FIU, Immigration and the Bureau of Public Safety. The Senate has recently refused to approve the re-nomination of the Chairman of the FIC, Daiziro Nakamura..

Palau has enacted several legislative mechanisms to foster international cooperation. The Mutual Assistance in Criminal Matters Act (MACA), passed in June 2001, enables authorities to cooperate with other jurisdictions in criminal enforcement actions related to money laundering and to share in seized assets. The Foreign Evidence Act of 2001 provides for the admissibility in civil and criminal proceedings of certain types of evidence obtained from a foreign State pursuant to a request by the Attorney General under the MACA. Under the Compact of Free Association with the United States, a full range of law enforcement cooperation is authorized and in 2004 Palau was able to assist the Department of Justice in a money laundering investigation by securing evidence critical to the case and freezing the suspected funds.

Pursuant to the adoption of the Asia/Pacific Group's (APG) mutual evaluation of Palau at its September 2003 Plenary, the Government of Palau (GOP) has proposed amendments to the MLPCA that, if enacted, would strengthen Palau's anti-money laundering regime. Among the more significant proposals are the following: the promulgation of reporting regulations for all covered financial institutions as well as alternative remittance providers; the requirement to obtain the identification of the beneficial owner of any type of account; mandatory reporting of suspicious transaction reports to the FIU regardless of the amount of the transaction; the requirement that any currency transaction over \$5000 be done by wire transfer; the requirement that alternative remittance systems providers report any cash remittance over \$500; and, a burden shifting regime for the seizure and forfeiture of assets upon a conviction for money laundering.

The President has also recently proposed the Cash Courier Act of 2004 that was drafted by the Palau Anti-Money Laundering Working Group.

The Omnibus Terrorism Act is currently pending in the OEK. If enacted with changes proposed by the President of the Republic, the Act would comport with current international standards, including provisions for the freezing of assets of entities and persons designated by the United Nations as

terrorists or terrorist organizations, provisions for the regulation of non-profit entities to prevent abuses by criminal organizations and terrorists and provisions for criminalizing the financing of terrorism. The OEK has issued resolutions ratifying Palau's accession to all the United Nation's Conventions and Protocols relating to terrorism.

The Government of Palau has taken several steps toward enacting a legal framework by which to combat money laundering. It has signed Pacific Island Forum anti-money laundering initiatives and as a member of the Asia/Pacific Group on Money Laundering, Palau is committed to implement the Financial Action Task Force Revised Forty Recommendations and its Nine Special Recommendations on Terrorist Financing. As a party to the UN Convention for the Suppression of the Financing of Terrorism, Palau should criminalize the financing of terrorism. In continuing its efforts to comport with international standards, Palau should enact legislation and promulgate implementing regulations to the MLPCA, as recommended by the APG, including but not limited to establishing funding for the FIU, eliminating the threshold for reporting suspicious transactions and beginning a broad-based implementation of the legal reforms already put in place.

## **Panama**

The economy of Panama is service-based and heavily weighted toward maritime transportation, commerce, tourism, banking, and financial services. Panama is a major drug-transit country. Panama's proximity to major drug-producing countries, its sophisticated international banking sector, its U.S. dollar-based economy, and the Colon Free Zone's (CFZ's) role as an originating or transshipment point for goods purchased with narcotics dollars through the Colombian Black Market Peso Exchange, make the country particularly vulnerable to money laundering. Despite significant progress to strengthen Panama's anti-money laundering regime since October 2000, money laundering remains a serious threat to the stability of the country's legitimate financial institutions. Panama is a destination for international narcotics-trafficking proceeds that include significant amounts of U.S. currency or currency derived from illegal drug sales in the United States.

Panama's large offshore financial sector includes international business companies (over 370,000 currently registered in Panama), offshore banks (approximately 31), captive insurance companies (corporate entities created and controlled by a parent company, professional association, or group of businesses), and trust companies. Transfer of negotiable (bearer) bonds is another potential vulnerability that could be exploited by money launderers. The high volume of trade occurring through the CFZ (there are approximately 2,600 businesses established in the Zone) presents opportunities for trade-based money laundering to occur.

Law No. 41 (Article 389) of October 2, 2000, amended the Penal Code by expanding the predicate offenses for money laundering beyond narcotics-trafficking, to include criminal fraud, arms trafficking, trafficking in humans, kidnapping, extortion, embezzlement, corruption of public officials, terrorism, and international theft or trafficking of motor vehicles. Law No. 41 establishes a punishment of five to 12 years imprisonment and a fine.

In December 2002, the Panamanian Legislative Assembly approved the Financial Crimes Bill (Law No. 6 of December 6, 2002), which establishes criminal penalties of up to ten years in prison and fines of up to one million dollars for financial crimes that undermine public trust in the banking system, the financial services sector, or the stock market. The penalties criminalize a wide range of activities related to financial intermediation, including the following: illicit transfers of monies, accounting fraud, insider trading, and the submission of fraudulent data to supervisory authorities. Law No. 1 of January 5, 2004, adds crimes against intellectual property as a predicate offense for money laundering.

Law No. 42 of October 2, 2000, requires financial institutions (banks, trust companies, money exchangers, credit unions, savings and loans associations, stock exchanges and brokerage firms, and investment administrators) to report to the Unidad de Analisis Financiero (UAF), Panama's Financial Intelligence Unit (FIU), currency transactions in excess of \$10,000 and suspicious financial transactions. Law 42 also mandates that casinos, CFZ businesses, the national lottery, real estate agencies and developers, and insurance/reinsurance companies report to the UAF currency or quasi-currency transactions that exceed \$10,000. Furthermore, Law 42 requires Panamanian trust

companies to identify to the Superintendence of Banks the real and ultimate beneficial owners of trusts.

Executive Order 213 of October 3, 2000, amending Executive Order 16 of 1984 relating to trust operations, provides for the dissemination of information related to trusts to appropriate administrative and judicial authorities. Furthermore, in October 2000, Panama's Superintendence of Banks issued Agreement No. 9-2000 that defines requirements that banks must follow for identification of customers, exercise of due diligence and retention of transaction records.

In 2002, the Ministry of Commerce and Industry issued a circular to all finance companies reminding them of the transaction-reporting requirement of Law 42, and also began drafting a law to regulate the operations of pawnshops and exchange houses. It also increased the number of inspections of finance companies it conducted. The Autonomous Panamanian Cooperative Institute established a specialized unit for the supervision of loans and credit cooperatives regarding compliance with the requirements of Law 42. The National Securities Commission carried out numerous training sessions and workshops for its personnel and regulated entities. The Colon Free Zone Administration prepared and issued a procedures manual for the users of the CFZ, outlining their responsibilities regarding prevention of money laundering and requirements under Law 42. The UAF continues efforts to raise the level of compliance for reporting suspicious financial transactions, particularly by non-bank financial institutions and businesses in the CFZ. In 2004, the Stock Commission announced that it would begin investigating suspicious activity.

With support from the Inter-American Development Bank, the GOP is implementing a Program for the Improvement of the Transparency and Integrity of the Financial System. This Transparency Program is targeted, through enhanced communication and information flow, training programs, and technology, at strengthening the capabilities of those government institutions responsible for preventing and combating financial crimes and terrorist financed activities.

In 2002, the Institute of Autonomous Panamanian Cooperatives, UAF, and the U.S. Embassy Narcotics Assistance Section cosponsored a roundtable on money laundering that offered practical training to financial institutions to assist them in meeting the reporting requirements under Law No. 42. In 2003, Panama launched an education program related to prevention of money laundering and terrorist financing. Panama's Banking Association, the Inter-American Development Bank, the Panamanian Government, and the United States Government financed this campaign. Initiatives under this campaign include a crime analysis seminar, a regional seminar on money laundering for banking regulators, and the detection and reporting of suspicious activities for the banking sector. During 2004, the programs included training for the Gaming Control Commission and a seminar for the Hemispheric Congress on the prevention of money laundering. In 2004, more than 5,000 officials from public and private sector institutions received training through this campaign. Participants included representatives from banks, credit unions, real estate agencies, stockbrokers, insurance companies, Colon Free Trade Zone companies, financial institutions, and money order companies.

To increase GOP interagency coordination, the UAF and Panamanian Customs are developing an office at the Tocumen International Airport to expedite the entry of customs currency declaration information into the UAF's database. This will enable the UAF to begin more timely investigations. In 2004, Panamanian Customs continued a program at Tocumen International Airport, begun in 2001, to deter currency smuggling by seizing and forfeiting all undeclared funds in excess of \$10,000 from arriving passengers. Bulk cash shipments, including through Tocumen Airport, continue to be of great concern, with smugglers often under-declaring the amount of cash being brought into the country.

Executive Order No. 163 of October 3, 2000, which amended the June 1995 decree that created the UAF, also allows the UAF to provide information related to possible money laundering directly to the Office of the Attorney General for investigation. Panama has brought cases for domestic prosecution, and the UAF routinely transfers cases to the Unidad de Inteligencia Financiera (UIF) for investigation. During 2004 the Financial Fraud Prosecutor's office investigated 2,459 cases related to financial crimes, 86 of which led to a conviction. These included credit card fraud and fraud involving banking institutions.



GOP cooperation in the investigation of the Western Hemisphere's largest Black Market Peso Exchange money laundering scheme was instrumental in the U.S. conviction in 2002 of Yardeni Hebroni, owner of Speed Joyeros, a CFZ enterprise. The GOP also revoked the Panamanian residency of Hebroni, an Israeli national, after she was ordered deported from the United States. In 2004, Panamanian officials charged former Nicaraguan President Arnoldo Aleman with money laundering crimes. The GOP received cooperation in the investigation from the Government of Nicaragua. Also during 2004, there were investigations into possible money laundering crimes of high-level Costa Rican government officials. Finally, GOP investigators are looking into corruption allegations made against former government officials.

The GOP identified the combating of money laundering as one of five goals in its five-year National Drug Control Strategy issued in 2002. The Strategy commits the GOP to devote \$2.3 million to anti-money laundering projects, the largest being institutional development of the UAF.

Decree No. 22 of June 2003, gave the Presidential High Level Commission against Narcotics Related Money Laundering responsibility for combating terrorist financing. Law No. 50 of July 2003 criminalizes terrorist financing and gives the UAF responsibility for prevention of this crime. There are no legal impediments to the GOP's ability to prosecute or extradite suspected terrorists. Panama Public Force (PPF) and the judicial system have limited resources to deter terrorists, due to insufficient personnel and lack of expertise in handling complex international investigations. On January 18, 2003, the GOP entered into a border security cooperation agreement with Colombia, and also increased funds to the PPF to help secure the frontier. In response to United States efforts to identify and block terrorist-related funds, the GOP continues to monitor suspicious financial transactions.

Also, the GOP created the Department of Analysis and Study of Terrorist Activities. This department is tasked with working with the United Nations and the Organization of American States to investigate transnational issues, including money laundering. Panama has an implementation plan for compliance with the Financial Action Task Force (FATF) Forty Recommendations on Money Laundering and its Special Recommendations on Terrorist Financing.

Panama and the United States have a Mutual Legal Assistance Treaty that entered into force in 1995. The GOP has also assisted numerous countries needing help in strengthening their anti-money laundering programs, including Guatemala, Costa Rica, Russia, Honduras, and Nicaragua. Panama also hosted the Seventh Hemispheric Congress on the Prevention of Money Laundering in August 2003. Executive Decree No. 163 authorizes the UAF to share information with FIUs of other countries, subject to entering into a memorandum of understanding or other information exchange agreement. The UAF has signed more than 27 memoranda of understandings with FIUs, including the U.S. FIU, FinCEN.

Panama is active in the multilateral Black Market Peso Exchange Group Directive. In March 2002, the GOP signed the cooperation agreement issued by the working group as part of a regional effort against the black market system. Panama is a member of the Organization of American States Inter-American Drug Abuse Control Commission (OAS/CICAD), and is the current Chair of the Caribbean Financial Action Task Force. Panama is also a member of the Offshore Group of Banking Supervisors, and the UAF is a member of the Egmont Group. Panama is a party to the 1988 UN Drug Convention. Panama is a signatory to 11 of the UN terrorism conventions and protocols. During 2002, the GOP became a party to the UN International Convention for the Suppression of the Financing of Terrorism, and in 2004, of the UN Convention against Transnational Organized Crime.

The Government of Panama should continue its regional assistance efforts. It should also continue implementing the significant reforms it has undertaken to its anti-money laundering regime, in order to reduce the vulnerability of Panama's financial sector and to enhance Panama's ability to investigate and prosecute financial crime, money laundering, and potential terrorist financing. In particular, Panama should institute controls over the transfer of bearer bonds.

## **Papua New Guinea**

Papua New Guinea is not a regional financial center. Its banking sector is relatively small. There are currently no laws against money laundering or terrorist financing. However, according to the

Government of Papua New Guinea's (GPNG's) September 2003 report to the UN Counter-Terrorism Committee that monitors implementation of UN Security Council Resolution 1373 (CTC) money laundering in Papua New Guinea will be criminalized pursuant to the proposed "Proceeds of Crime Bill." The bill would obligate financial institutions to retain essential financial documents for a specific period of time. Covered transactions will include transmission of funds between Papua New Guinea and a foreign country. The proposed legislation also calls for the communication of suspicious information by financial institutions to the police.

The GPNG continues to consider amending the Criminal Code Act that will cover the collection, recruiting, or soliciting of funds from other countries for terrorists/terrorist purposes. In addition, the National Intelligence Organization (NIO) is in the process of submitting a Plan of Action on counterterrorism and other transnational crimes. The Plan of Action will focus on coordination and sharing of intelligence. Currently interagency coordination does exist to some extent with regard to narcotics, and task force "Centre-points" have also been established to monitor and share intelligence information on drug trafficking, arms smuggling, human trafficking, and other border concerns. However, "financial tracking" is not yet fully developed.

Papua New Guinea is not a party to any bilateral or multilateral treaties on mutual assistance in criminal matters. Reportedly, the GPNG plans legislation in this area. Papua New Guinea is an observer to the Asia/Pacific Group on Money Laundering. The GPNG is not a party to the 1988 UN Drug Convention but is a party to the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Papua New Guinea should enact a comprehensive anti-money laundering regime that criminalizes money laundering related to all serious crimes. Specific counterterrorism legislation implementing UNSCR 1373 and the UN International Convention for the Suppression of the Financing of Terrorism should also be adopted, including criminalizing terrorism and the funding of terrorism. Papua New Guinea should also become a party to the 1988 UN Drug Convention. Papua New Guinea should become a member of the Asia/Pacific Group on Money Laundering.

## **Paraguay**

Paraguay is a principal money laundering center, involving both the banking and non-banking financial sectors. The multi-billion dollar contraband re-export trade that occurs largely on the border shared with Argentina and Brazil facilitates much of the money laundering in Paraguay. Paraguay is a major drug-transit country. The Government of Paraguay (GOP) suspects that proceeds from narcotics-trafficking are often laundered, but is it difficult to determine what percentage of laundered funds is directly generated from narcotics sales. Weak controls in the financial sector, an open border, and minimal enforcement activity for financial crimes allow money launderers and terrorist financiers to take advantage of Paraguay's financial system. Although the Government of Paraguay (GOP) has made some progress in 2004, it will need to pursue more aggressive policies in 2005 in order to increase its effectiveness in combating money laundering and terrorist financing.

Paraguay is particularly vulnerable to money laundering, as little personal background information is required to open a bank account or to make financial transactions in Paraguay. Paraguay is an attractive financial center for neighboring countries, particularly Brazil. Foreign banks are registered in Paraguay and nonresidents are allowed to hold bank accounts, but current regulations forbid banks from advertising or seeking deposits from outside the country. Paraguay is not considered to be an offshore financial center, but the GOP does allow representative offices of offshore banks to maintain a presence in the country. Shell companies are not permitted; trusts, however, are permitted and are regulated by the Central Bank. The Superintendent of Banks audits financial institutions and supervises all banks under the same rules and regulations. However, there are few effective controls over businesses, and a large informal economy exists outside the regulatory scope of the GOP.

Money laundering in Paraguay is facilitated by the multi-billion dollar contraband re-export trade that occurs largely in the Triborder Area shared by Paraguay, Argentina, and Brazil. Ciudad del Este (CDE), on the border between Brazil and Paraguay, represents the heart of Paraguay's informal economy. The area is well known for arms and narcotics-trafficking, as well as crimes against intellectual property rights. A wide variety of counterfeit goods, including cigarettes, CDs, DVDs, and

computer software, are imported from Asia and transported primarily across the border into Brazil, with a significantly smaller amount remaining in Paraguay for sale in the local economy. Some senior government officials, including members of Congress, have been accused of involvement in the smuggling of contraband or pirated goods. To date there have been few criminal investigations, much less prosecutions of senior GOP officials involvement in smuggling contraband or pirated goods) Government officials, in both Paraguay and the United States, also suspect the area to be a source of terrorist financing. Raids in CDE have led to the seizure of extremist Islamic materials and receipts of wire transfers from Paraguay to the Middle East and the United States. Paraguay has taken some measures to tackle this "gray" economy and to develop strategies to implement a formal, diversified economy.

In 2003 the GOP noted that it was trying to introduce "maquilas" (assembly line industries) but had not done so in 2004. The GOP is trying to strengthen its tourism industry by proposing advances to its tourism infrastructure such as the international airport in Asuncion, making it a regional transportation hub for cargo and possibly passenger airlines.) Although currently no formal free trade zones are located within the country, the new customs code implemented in early 2004 provides for the creation of these zones. One is currently being planned in the town of Villeta, near Asunción. These free trade zones will not help reduce money laundering in Paraguay-in fact, the addition of free trade zones may provide additional venues for money laundering.

There are no effective controls on the amount of currency that can be brought into or out of Paraguay. Cross-border reporting requirements are limited to those issued by airlines at the time of entry into Paraguay. Persons transporting \$10,000 into or out of Paraguay are required to file a customs report, but these reports are often not actually collected or checked. Customs operations at the airports or land ports of entry provide no control of the cross-border movement of cash. The non-bank financial sector, particularly exchange houses, are used to move illegal proceeds both from within and outside of Paraguay into the formal banking system of the United States. Most of these funds move from Brazil through Ciudad del Este to the banking sector. Paraguay exercises a dual monetary system in which most high-priced goods are paid for in U.S. dollars. Large sums of dollars generated from normal commercial activity and suspected illicit commercial activity are transported physically from Paraguay through Uruguay to the banking centers in the United States. Within the past year, the GOP has begun to recognize and address the problem of the international transportation of currency and monetary instruments derived from illegal sources.

Bank fraud, which has led to several bank failures, and other financial crimes related to corruption are serious problems in Paraguay. Following bank failures in 2002 and 2003, Paraguay continues to experience problems in the banking industry. In 2004, Citibank decided to end its participation in small-consumer banking in Paraguay, and subsequently closed almost all of its branches nationwide. The GOP continues to work with the U.S. Treasury and Justice Departments to trace, account for, and return the missing \$16 million diverted from the Central Bank in 2002 to private accounts allegedly linked to the family of former President Luis Gonzalez Macchi.

Money laundering is a criminal offense under Paraguay's two anti-money laundering statutes, Law 1015 of 1996 and Article 196 of Paraguay's Criminal Code, adopted in 1997. The existence of the two laws has led to substantial confusion due to overlapping provisions. Under Article 196, the scope of predicate offenses includes only offenses that carry a maximum penalty of five years or more; Law 1015 includes additional offenses. Article 196 also establishes a maximum penalty of five years for money laundering offenses, while Law 1015 carries a prison term of two to ten years. This is particularly significant because, under the new Criminal Code and Criminal Procedure Code, defendants who accept charges that carry a maximum penalty of five years or less are automatically entitled to a suspended sentence and a fine instead of jail time, at least for the first offense. Since a defendant cannot be charged with money laundering unless he or she has first been convicted of the predicate offense, many judges are apparently reluctant to prosecute any defendant on money laundering charges because a sentence has already been issued for a predicate offense.

Law 1015 of 1996 also contains "due diligence" and "banker negligence" provisions and applies money laundering controls to non-banking financial institutions, such as exchange houses. Bank secrecy laws do not prevent banks and financial institutions from disclosing information to bank

supervisors and law enforcement entities. Additionally, bankers and others are protected under the anti-money laundering law with respect to their cooperation with law enforcement agencies.

Additional provisions of Law 1015 require banks and financial institutions to know and record the identity of customers engaging in significant currency transactions and to report those, as well as suspicious activities, to Paraguay's Financial Intelligence Unit (FIU), the Unidad de Análisis Financiera (UAF). The UAF began operating in 1997 within the Secretary for the Prevention of Money Laundering (SEPRELAD), under the auspices of the Ministry of Industry and Commerce (MIC). However, for many years the UAF had been regarded as ineffective, and was hampered by a burdensome bureaucratic structure, lack of financial support, and the inability to keep trained personnel.

The UAF's weaknesses were reflected in the small number of cases presented to the Public Ministry (Attorney General's office) for prosecution. Before 2001, only one case went to trial, and it was dismissed on procedural grounds. The majority of the cases prepared by the UAF were incomplete and were returned to the UAF by prosecutors for more information or investigation. Serious concerns also exist with regard to UAF's personnel, its handling of confidential information, cumbersome record keeping, and concerns about possible corruption within the FIU. Efforts were made to by the GOP to improve its anti-money laundering capabilities, and in 2003, existing personnel began to be vetted and replaced as appropriate. However, there remains limited exchange of information between U.S. law enforcement agencies and GOP entities on money laundering cases, as a result of a leak of information in 2002. Information is now exchanged on a case-by-case basis.

The banking "Risk Control Division," created in 2003 to replace the Superintendent of Banks' FIU, and eliminate its duplicative function with the UAF, has the primary responsibility of reviewing the records of national financial institutions for suspected terrorist activity. The Risk Control Division is empowered to coordinate information exchange with the Central Banks of other MERCOSUR countries, but has no authority to conduct investigative work associated with financial suspicious activity reports. That remains the purview of the UAF. According to SEPRELAD officials, there has been little coordination or cooperation between the UAF and the Risk Control Division. The two groups are collaborating on a memorandum of understanding (MOU), which will lay out the provisions for increased cooperation. The MOU is scheduled to come into effect early this year. In 2004, the RCD suffered some growing pains, since its inception last year, and is off to a slow start. The division is working on several *casas de cambio* cases among its current caseload. )

In 2004 SEPRELAD made significant efforts to improve the UAF's personnel, analytical capabilities, infrastructure, and technical capabilities. All UAF personnel are now vetted and receive significant analytical training. The UAF is seeking to strengthen its relationship with other financial intelligence units; for example, the UAF is working with the U.S. financial intelligence unit, FinCEN, to re-establish information sharing procedures, which were suspended following an unauthorized disclosure by the GOP of U.S. financial information in 2001. In 2004, SEPRELAD helped to create and coordinate an interagency money laundering working group, whose members include the director of the UAF, the director of the National Anti-Drug Secretariat (SENAD), the assistant attorney general for economic crimes, the director of the customs agency and a criminal appellate judge.

The UAF also increased its role in regional and international anti-money laundering groups, including the Egmont Group and the Financial Action Task Force for South America (GAFISUD). The UAF's director now participates in the GAFISUD FIU Working Group and a committee within the Egmont Group, further expanding Paraguay's role in these organizations. Paraguay will undergo its second mutual evaluation by GAFISUD in 2005.

The new law to improve the effectiveness of Paraguay's anti-money laundering regime, drafted in late 2003, was formally introduced to Congress in May 2004, where it now remains under consideration by legislative committees. The draft law should come before the full Congress for consideration in 2005. The GOP is also in the process of drafting an counterterrorism bill to address terrorist financing issues.

The new money laundering legislation, if approved, will institute important national reforms. In addition to confirming the UAF's role as the sole FIU, it establishes SEPRELAD an independent secretariat or agency reporting directly to the Office of the President. The draft law also establishes money laundering as an autonomous crime punishable by a prison term of five to 20 years. It establishes

predicate offenses as any crimes that are punishable by a prison term exceeding six months, and specifically criminalizes money laundering tied to the financing of terrorist groups or acts. The full range of covered institutions will be required to report suspicious transactions to the UAF and to maintain registries of large currency transactions that equal or exceed \$10,000. Under the draft legislation, those institutions have been expanded to include, inter alia, banks; financial institutions; insurance agencies; currency exchange houses; securities companies and brokers (stock exchange); investment companies; money transmitters; administrators of mutual investment and pension funds; credit unions; operators of gambling facilities; real estate agencies; nongovernmental organizations; pawnshops; and dealers in jewels, precious stones and metals, automobiles, art, and antiques. Other provisions of the draft law include penalties for failure to file or falsify reports, "know-your-client provisions," and standardized record keeping for a minimum of seven years. The UAF will continue to refer cases as appropriate for further police (SENAD) investigation and to the Attorney General's Office for prosecution. It will also serve as the central entity for related information exchanges with other concerned foreign entities. The law further specifies that the investigative unit of SENAD is the principal authority for carrying out all counternarcotics and other financial investigations, and will also have the authority to initiate investigation of cases on its own.

There are other challenges, however, that the new money laundering legislation, when passed, will not address. With only eight prosecutors dedicated to financial crimes, Paraguay currently has limited resources to investigate and prosecute money laundering and financial crimes. Moreover, prosecutors have little experience working with the UAF, and unless the new law is enacted, most judges have little incentive to investigate money laundering cases because many believe that sentencing on predicate offenses is sufficient punishment. Thus, there have not been any successful money laundering prosecutions in Paraguay so far, and improvement is unlikely until the new law becomes a reality. As it is, those individuals implicated in money laundering are prosecuted on tax evasion charges. In May 2004, Assad Barakat—widely alleged to be involved in money laundering—was convicted of tax evasion and sentenced to six and one-half years in prison. In late 2004, prosecutors were investigating several tax evasion cases involving suspected money laundering by both legal and illegal money exchange offices in Ciudad del Este.

Another serious problem for money laundering investigations that will not be corrected by the new law is the obligation of federal prosecutors to notify a suspect in writing that he/she is the subject of an investigation. Suspects must be notified within six months of the start of an investigation, and may have access to all information gathered through the investigation. This is mandated by Paraguay's penal code.

Under current laws, the GOP has limited authority to freeze, seize, and/or forfeit assets of suspected money launderers. In most cases, assets that the GOP is permitted to freeze, seize, and/or forfeit are limited to transport vehicles, such as planes and cars, and normally do not include bank accounts. However, authorities may not auction off these assets until a conviction is announced by the judicial system. At best, the GOP can establish a "preventative embargo" against assets of persons under investigation for a crime in which the state risks loss of revenue from furtherance of a criminal act, such as tax evasion. However, in those cases the limit of the embargo is set as the amount of liability of the suspect to the government. As the government entity primarily responsible for the tracing and seizing of assets, SENAD is required to split the proceeds of the forfeiture with the Public Ministry. SENAD currently has no figure for the amount of assets seized and/or forfeited in 2004, as it does not place a value on these assets before auction. Under current provisions of the law, significant legal loopholes exist, allowing criminals to hide their assets under another person's name.

The new anti-money laundering legislation will, when passed, allow prosecutors to recommend that judges freeze or confiscate assets connected to money laundering and its predicate offenses. The draft law also provides for the creation of a special asset forfeiture fund to be administered by a consortium of national governmental agencies, which will support programs for crime prevention and suppression, including combating money laundering, and related training.

The GOP currently has no authority to freeze, seize, and/or forfeit assets related to the financing of terrorism. A recent attempt to freeze the assets of a suspected terrorist financier for tax evasion failed because prosecutors perceived that the Paraguayan constitution prohibits the confiscation of personal property. The financing of terrorism is not criminalized under current Paraguayan law. However, the

Ministry of Foreign Affairs often provides the Central Bank and other government entities with a list of groups or individuals included on the UNSCR 1267 Sanctions Committee consolidated list; to date, the GOP has not identified, seized, or forfeited any such assets linked to these groups or individuals. The current law also does not provide any measures for thwarting the misuse of charitable or non-profit entities that can be used as conduits for the financing of terrorism. Following the submission of the draft anti-money laundering law to Congress in May 2004, a working group of GOP and U.S. officials began drafting legislation to address terrorism and terrorist financing. The draft legislation will allow the GOP to conform to international standards on the suppression of terrorist financing. The draft anti-money laundering legislation will also specifically criminalize money laundering tied to the financing of terrorist groups or acts.

The GOP ratified the UN International Convention for the Suppression of the Financing of Terrorism in November 2004 and the Organization of American States Inter-American Convention on Terrorism in January 2005. Paraguay has also signed, but not ratified, the UN Convention against Corruption. In September 2004, the GOP ratified the UN Convention against Transnational Organized Crime. Paraguay is party to the 1988 UN Drug Convention, and participates in Summit of the Americas and Inter-American Drug Abuse Control Commission (CICAD)-related meetings on money laundering. Paraguay is a member of the South American Financial Action Task Force (GAFISUD), the Egmont Group, and the "3 Plus 1" Counter-Terrorism Dialogue between the United States and the Triborder Area countries.

While the Government of Paraguay took a number of positive steps in 2004, there are other initiatives that should be pursued in 2005 to increase the effectiveness of Paraguay's efforts to combat money laundering and terrorist financing. Most important is enactment of the new money laundering law that meets international standards. Paraguay should also continue efforts to combat corruption, and increase information sharing among concerned agencies when and if the corruption issues are resolved. Paraguay does not have a counterterrorism law or a law criminalizing terrorist financing. While the new money laundering law would increase the Government of Paraguay's abilities to combat terrorist financing, it should also take steps as quickly as possible to ensure that comprehensive counterterrorism legislation is passed. Reforms to the criminal procedure code that would allow prosecutors to carry out long-term criminal investigations should be considered. Reforms to the customs agency are also necessary in order to allow for increased inspections and interdictions at ports of entry and to develop strategies targeting the physical movement of bulk cash. It is essential that the Unidad de Análisis Financiera continue to receive the financial and human resources necessary to operate as an effective, fully functioning Financial Intelligence Unit capable of effectively combating money laundering, terrorist financing, and other financial crimes.

## **Peru**

Peru is not a major regional financial center, nor is it an offshore money laundering haven. Peru is a major drug producing and drug-transit country. Narcotics-related and other money laundering does occur, and the Government of Peru (GOP) has taken several steps to improve its money laundering legislation and enforcement abilities. Nevertheless, more effort is necessary to better assess the scale and methodology of money laundering in Peru. Peru is the world's second largest producer of cocaine, and, although no reliable figures exist regarding the exact size of the narcotics market in Peru, conservative estimates indicate that the cocaine trade generates between 1.5 to two billion dollars per year. As a result, money laundering occurs on a significant scale to integrate the illegal proceeds generated from the cocaine trade into the Peruvian economy.

Money laundering has historically been facilitated by a number of factors. Peru's economy is heavily dependent upon the U.S. dollar and approximately 65 percent of the economy is dollarized, allowing traffickers to handle large bulk shipments of U.S. currency with minimal complications. Currently no restrictions exist on the amount of foreign currency an individual can exchange or hold in a personal account, and until recently, there were no controls on bulk cash shipments coming into Peru.

A number of former government officials, most from the Fujimori administration, are under investigation for corruption-related crimes, including money laundering. These officials have been accused of transferring tens of millions of dollars in proceeds from illicit activities (e.g., bribes, kickbacks, or protection money) into offshore accounts in the Cayman Islands, the United States,

and/or Switzerland. The Peruvian Attorney General, a Special Prosecutor, the office of the Superintendent of Banks (SBS) and the Peruvian Congress have conducted numerous investigations, some of which are ongoing, involving dozens of former GOP officials. In 2004, the GOP continued to make strong efforts at uncovering and recovering the millions of U.S. dollars believed to be the proceeds of money laundering activities carried out by Vladimiro Montesinos, former director of the Peruvian National Intelligence Service. However, there have been no convictions for money laundering offenses to date in Peru.

On June 1, 2004, the United States Department of the Treasury's Office for Foreign Assets Control (OFAC) initiated an investigation of Fernando Zevallos Gonzales, founder and de facto owner of Peru's largest airline, Aero Continente. Because of Zevallos's suspected links to narcotics-trafficking and money laundering, all of his assets in the United States were frozen by OFAC. OFAC formally added Aero Continente, now known as Nuevo Continente, to its Specially Designated Nationals (SDN) list pursuant to the Foreign Narcotics Kingpin Designation Act.

Prior to 2002, Peru had a relatively weak anti-money laundering legislative and regulatory framework. The previous system criminalized only the laundering of proceeds directly associated with narcotics trafficking and "narcoterrorism," and mandated that all unusual or suspicious financial transactions be reported directly to the Public Ministry. Only banks and other financial institutions were required to report suspicious transactions or large cash transactions, and the requirement to report cash transactions was suspended in August 1998, one month after it went into effect.

In 2002, the GOP strengthened its anti-money laundering regime by creating a Financial Intelligence Unit (FIU), expanding the type of institutions required to file suspicious transaction reports, increasing the number of predicate crimes, criminalizing willful blindness, and reinstating reporting requirements for large cash transactions. In April and June of that year, Laws 27.693 and 27.765 were adopted. Law 27.765 expands the predicate offenses for money laundering to include the laundering of assets related to all serious crimes, such as narcotics-trafficking, terrorism, corruption, trafficking of persons, and kidnapping.

The penalties for money laundering were also revised. Instead of a life sentence for the crime of laundering money, Law 27.765 sets prison terms of up to 15 years for convicted launderers, with a minimum sentence of 25 years for cases linked to narcotics-trafficking, terrorism, and laundering through banks or financial institutions. In addition, revisions to the Penal Code criminalize "willful blindness," the failure to report money laundering conducted through one's financial institution when one has knowledge of the money's illegal source, and imposes a three to six year sentence for failure to file suspicious transaction reports.

Law 27.693 provided for the creation of Peru's financial intelligence unit, the Unidad de Inteligencia Financiera (UIF), an autonomous body reporting to the Office of the Prime Minister. The law also expanded the entities obligated to report suspicious transactions beyond just banks and financial institutions. Stock funds or brokers, credit and debit card companies, exchange houses, mail and courier services, travel and tourism agencies, hotels and restaurants, notaries, the customs agency, casinos, auto dealers, construction or real estate firms, and other sectors, in addition to banks and financial institutions, are all required to report suspicious transactions to the UIF within 30 days.

These entities are required to maintain registries of suspicious transaction reports (STRs) sent to the UIF. Law 27.693 also reinstated reporting requirements for large cash transactions, and requires the reporting of individual cash transactions exceeding \$10,000 or transactions totaling \$50,000 in one month. Nonfinancial institutions, such as exchange houses, casinos, lotteries or others, must report individual transactions over \$2,500 or monthly transactions over \$10,000. These cash transaction reports (CTRs) must be maintained in internal databases for a minimum of five years and be made available to the UIF upon request. Major institutions are required to appoint supervisory-level compliance officials to ensure that all reporting requirements for STRs and CTRs are met.

Law 27.693 also enables the UIF to request information from the following entities: the National Superintendence for Tax Administration, Customs, the Securities and Exchange Commission, the Public Records Office, the Public or Private Risk Information Centers, and the National Identification

Registry and Vital Statistics Office. However, the UIF can only share information with other agencies—including foreign entities—if there is a joint investigation underway.

In July 2004, the GOP demonstrated further efforts to strengthen its anti-money laundering and terrorist financing system with the passage of Law 28.306. Law 28.306, which entered into effect on July 30, 2004, mandated that covered entities report suspicious transactions related to terrorist financing, and expanded the UIF's functions to include the ability to analyze reports related to terrorist financing. Terrorist financing is criminalized under Executive Order 25.475, but Law 27.693 did not require covered entities to report suspicious transactions related to the financing of terrorism, nor did it enable the UIF to analyze such reports.

Law 28.306 also increased the number of individuals and entities required to file CTRs or STRs and expanded the number of government agencies from which the UIF may request information. A new reporting requirement was added as well: individuals or entities transporting more than \$10,000 in currency or monetary instruments into or out of Peru must file reports with the customs agency, and the UIF may have access to those reports upon request. The law also gives the UIF the power to sanction entities for failure to report suspicious transactions, large cash transactions, or the transportation of currency or monetary instruments. Under Law 28.306, the UIF now has regulatory responsibilities for all covered entities that do not fall under the supervision of another regulatory body (such as the Superintendence of Banks).

The UIF began operations in June 2003 and today has 41 personnel. Reporting requirements entered into effect in September 2003, and as of October 2004 the UIF has received approximately 190 STRs. The FIU cannot receive STRs electronically; covered entities must hand-deliver STRs to the UIF.

The UIF has requested additional information from the covered entities on roughly 30 percent of the STRs. The UIF currently does not receive cash transactions reports or reports on the international transportation of currency or monetary instruments. CTRs are maintained in internal registries within the obligated entities, and reports on the international transportation of currency or monetary instruments are maintained by the customs agency. If the UIF receives an STR and determines that the STR warrants further analysis, it contacts the covered entity that filed the report for additional background information—including any CTRs that may have been filed—and/or the customs agency to determine if the subject of the STR had reported the transportation of currency or monetary instruments.

The UIF cannot receive CTRs without specifically requesting them from the covered entities, and there is no regular CTR reporting. Some requests for reports of transactions over \$10,000—such as those that are deposits into savings accounts—are protected under the constitution by bank secrecy provisions and require an order from the Public Ministry or SUNAT, the tax authority. A period of 15-30 days is required to lift the bank secrecy restrictions. All other types of cash transaction reports, however, may be requested directly from the reporting institution.

Once the UIF has completed the analysis process and determined that a case warrants further investigation or prosecution, the case is sent to the Public Ministry. Within the counternarcotics section of the Public Ministry, two specialized prosecutors are responsible for dealing with money laundering cases. As of December 2004, 19 cases had been sent to the Public Ministry for further investigation and all have been investigated by the two prosecutors. However, only three are ready for trial, and there have been no money laundering prosecutions in Peru to date.

In addition to being able to request any additional information from the UIF in their investigations, the Public Ministry may also request the assistance of the Directorate of Counternarcotics (DINANDRO) of the Peruvian National Police. With the passage of Law 28.306 in July 2004, DINANDRO and the UIF are now able to collaborate on investigations, although each agency must go through the Public Ministry in order to do so. DINANDRO may provide the UIF with intelligence for the cases the UIF is analyzing, while it provides the Public Ministry with assistance on cases that have been sent to the Public Ministry by the UIF.

The UIF was given regulatory responsibilities in July 2004 under Law 28.306. Most covered entities fall under the supervision of the Superintendence of Banks and Insurance (banks, the insurance sector,



financial institutions), the Peruvian Securities and Exchange Commission (securities, bonds), and the Ministry of Tourism (casinos). All entities that are not supervised by these three regulatory bodies, such as auto dealers, construction and real estate firms, etc., fall under the supervision of the UIF.

However, some covered entities remain unsupervised. For instance, although money remittance businesses are regulated by the Superintendence of Banks, the Superintendence is not required to supervise any money remittance business that does less than 1,240,000 soles (about \$400,000) in transfers per year. There is also difficulty in regulating casinos, as roughly 60 percent of that sector is informal. An assessment of the gaming industry conducted by GOP and U.S. officials in 2004 identified alarming deficiencies in oversight, and described an industry that is vulnerable to being used to launder large volumes of cash. Approximately 580 slot houses operate in Peru, with less than 65 percent or so paying taxes. Estimates indicate that under 42 percent of the actual income earned is being reported, while official gaming revenues totaled \$650 million in 2003. This billion-dollar cash industry continues to operate with little supervision.

Peru currently lacks comprehensive and effective asset forfeiture legislation. The Financial Investigative Office of DINANDRO has seized numerous properties over the last several years, but few were turned over to the police to support counternarcotics efforts. While Peruvian law does provide for asset forfeiture in money laundering cases, and these funds can be used in part to finance the UIF, no clear mechanism exists to distribute seized assets among government agencies. The government's "Fedadoi" fund currently holds around \$75 million in monies recovered after having been stolen or diverted during the Fujimori administration.

As one of four countries participating in the G-8 Anti-Corruption and Transparency initiative, the GOP has committed itself to create a specialized office within the Public Ministry to provide advice on locating and recovering stolen public assets. Also as part of the initiative, the UIF will pursue activities to raise public awareness of money laundering, research money laundering trends in specific sectors of the economy, further improve the legal framework addressing money laundering, and promote better GOP interagency cooperation in pursuing cases.

Terrorism is considered a problem in Peru, which is home to the terrorist organization Shining Path. Although the Shining Path has been designated by the United States as a foreign terrorist organization pursuant to Section 219 of the Immigration and Nationality Act and under Executive Order (E.O.) 13224, and the United States and 100 other countries have issued freezing orders against its assets, the GOP has no legal authority to quickly and administratively seize or freeze terrorist assets. In the event that such assets are identified, the Superintendent for Banks must petition a judge to seize or freeze them. A final judicial decision is then needed to dispose of or use such assets.

Foreign Ministry Officials are working with other GOP agencies to complete the necessary legal revisions that will permit asset-freezing actions. The Office of the Superintendent of Banks routinely circulates to all financial institutions in Peru updated lists of individuals and entities that have been included on the UNSCR 1267 Sanctions Committee's consolidated list as being linked to Usama Bin Ladin, the Taliban, and al-Qaida, as well as those on the list of Specially Designated Global Terrorist Entities designated by the United States pursuant to E.O. 13224 (on terrorist financing). To date, no assets connected to designated individuals or entities have been identified, frozen, or seized.

Peru also has not yet taken any actions to thwart the misuse of charitable or non-profit entities that can be used as conduits for the financing of terrorism. However, with the passage of Law 28.306, the GOP did make some improvements with regard to terrorist financing legislation in 2004. Law 28.306 mandates that covered entities report suspicious transactions related to terrorist financing, and enables the UIF to analyze those reports. The financing of terrorism is criminalized under Executive Order 25.475.

Peru ratified the UN International Convention for the Suppression of the Financing of Terrorism on November 10, 2001, and the Organization of American States Inter-American Convention on Terrorism in 2003. Peru is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime, and ratified the UN Convention against Corruption in November 2004. Peru is a member of the Organization of American States Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. Peru is also a member of the South

American Financial Action Task Force (GAFISUD), and was elected in July 2004 to hold the GAFISUD presidency in 2005. Peru is expected to become a member of the Egmont group of international FIUs in mid-2005. An extradition treaty between the U.S. Government and the GOP entered into force in 2003.

The Government of Peru has made serious advances in strengthening its anti-money laundering regime in 2004. However, some progress is still required. Anticorruption efforts in Peru should be a priority, and the need for strong confidentiality protocols for the Unidad de Inteligencia Financiera should be stressed. However, there are still a number of weaknesses in Peru's anti-money laundering system: bank secrecy must be lifted in order for the Unidad de Inteligencia Financiera to have access to certain cash transaction reports, smaller financial institutions are not regulated, and the Unidad de Inteligencia Financiera is not able to work directly with law enforcement agencies; rather, the Public Ministry must coordinate any collaboration between the Unidad de Inteligencia Financiera and the other agency. Peru should also enact legislation that allows for administrative as well as judicial blocking of terrorist assets. These issues should be addressed in order to strengthen Peru's ability to combat money laundering and terrorist financing.

## **Philippines**

The Philippines is a regional financial center. In the past few years, the illegal drug trade in the Philippines reportedly has evolved into a billion-dollar industry. The Philippines continues to experience an increase in foreign organized criminal activity from China, Hong Kong, and Taiwan. Insurgency groups operating in the Philippines fund their activities, in part, through the trafficking of narcotics and arms and engage in money laundering through alleged ties to organized crime. The proceeds of corrupt activities by government officials are also a source of laundered funds.

In June 2000, the Financial Action Task Force (FATF) placed the Philippines on its list of Non-Cooperative Countries and Territories (NCCT) for lacking basic anti-money laundering regulations, including customer identification and record keeping requirements, and excessive bank secrecy provisions. Following its placement on the NCCT list, the U.S. Government issued an advisory to all U.S. financial institutions instructing them to give "enhanced scrutiny" to transactions involving the Philippines.

The Government of the Republic of the Philippines (GRP) initially established an anti-money laundering and counterterrorist financing regime by passing the Anti-Money Laundering Act of 2001 (AMLA). The GRP enacted Implementing Rules and Regulations (IRR) for the AMLA in April 2002. The AMLA criminalized money laundering, an offense defined to include the conduct of activity involving the proceeds from unlawful activity in any one of 14 major categories of crimes, and imposes penalties that include a term of imprisonment of up to 14 years and a fine no less than 3,000,000 pesos (\$54,000) but no more than twice the value or property involved in the offense. The Act also imposed identification, record keeping and reporting requirements on banks, trusts and other institutions regulated by the Central Bank, insurance companies, securities dealers, foreign exchange dealers and money remitters, as well as any other entity dealing in valuable objects or cash substitutes regulated by the Securities and Exchange Commission.

The AMLA also established the Anti-Money Laundering Council (AMLC) as the country's Financial Intelligence Unit (FIU). The Council is composed of the Governor of the Central Bank, the Commissioner of the Insurance Commission, and the Chairman of the Securities and Exchange Commission. By law, the AMLC Secretariat is an independent agency responsible for receiving, maintaining, analyzing, and evaluating covered and suspicious transactions. It provides advice and assistance to relevant authorities and issues relevant publications. The AMLC's responsibilities include the investigation and prosecution of money laundering. AMLC has the ability to seize terrorist assets involved in money laundering on behalf of the Republic of the Philippines after a money laundering offense has been proven beyond a reasonable doubt. In order to freeze assets allegedly connected to money laundering, the AMLC must establish probable cause that the funds relate to an offense enumerated in the Act, such as terrorism. The Court of Appeals then may freeze the bank account for 20 days. The AMLC may apply to extend a freeze order prior to its expiration. The AMLC is required to obtain a court order to examine bank records for activities not listed in the Act, except for certain serious offenses such as kidnapping for ransom, drugs, and terrorism-related crimes. The AMLC and

the courts are working to shorten the time needed so funds are not withdrawn before the freeze order is obtained. The AMLC has finalized, and will soon issue, implementing regulations on the forfeiture of assets related to money laundering, including provisions for third party claims.

However, the Financial Action Task Force (FATF) deemed the original legislation inadequate and pressured the Philippines to amend the legislation to be more in line with international standards. The Government of the Republic of the Philippines (GRP) subsequently made important progress in developing its anti-money laundering and terrorist financing regime, with the enactment of amendments to the Anti-Money Laundering Act of 2001 (AMLA) in March 2003. The FATF deemed those amendments to have sufficiently addressed the main legal deficiencies in the original Philippines anti-money laundering regime, and decided not to apply any formal countermeasures.

The major purposes of the amendments to the AMLA are the following: to lower the threshold amount for covered transactions (cash or other equivalent monetary instrument) from 4,000,000 pesos to 500,000 pesos (\$80,000 to \$10,000) within one banking day; to expand financial institution reporting requirements to include the reporting of suspicious transactions, regardless of amount; to authorize the Central Bank (Bangko Sentral ng Pilipinas or BSP) to examine any particular deposit or investment with any bank or non-bank institution in the course of a periodic or special examination (in accordance with the rules of examination of the BSP), to ensure institutional compliance with the Anti-Money Laundering Act; and, to delete the prohibitions against the Anti-Money Laundering Council's examining particular deposits or investments opened or created before the Act. The AMLC is now able to respond to a request from foreign authorities regarding deposits and investments made prior to the coming into effect of the AMLA.

Over the last year, the Philippines also made progress in tracking, seizing, and blocking terrorist assets. The AMLC completed the first phase of its information technology upgrades in 2004. This is a significant milestone that allowed AMLC to electronically receive, store, and search CTRs filed by regulated institutions. Through 2004, the AMLC had received well over six hundred suspicious transaction reports (STRs) involving 5,451 suspicious transactions, and had received covered transaction reports (CTR) involving over 22 million covered transactions. In October 2004, the FATF met with the Philippines during the Asia/Pacific Review Group on Money Laundering to discuss progress addressing the remaining vulnerabilities. A FATF team conducted an on-site visit to the Philippines in January 2005 in order to determine if effective implementation of the AML reforms has taken place.

The Philippines is a member of the Asia/Pacific Group on Money Laundering. It is a party to the 1988 UN Drug Convention. The GRP has signed and ratified all 12 international conventions and protocols related to terrorism, including the UN Convention against Transnational Organized Crime (2002) and the UN International Convention for the Suppression of the Financing of Terrorism (2004). The Anti-Money Laundering Council is able to freeze funds and transactions identified with or traced to designated terrorist organizations or individuals upon request of the United Nations Security Council, the United States, and other foreign governments. The AMLC has responded to numerous requests for assistance from the U.S. and other countries. In a recent joint corruption investigation, conducted by U.S. and Philippine law enforcement, Philippine authorities expeditiously identified and froze over 40 accounts containing in excess of \$1 million total. Its follow-up investigations identified more accounts in the United States that were subsequently pursued by U.S. authorities (the Philippines and the U.S. have a Mutual Legal Assistance Treaty that entered into force in 1996). The United Kingdom recently praised the AMLC for assisting in the identification and repatriation of proceeds from money laundering. A number of money laundering related investigations are underway, most of which involve a failure to report covered transactions. In addition, a number of money laundering related cases are currently being heard a different regional trial courts throughout the Philippines.

In 2004, for the third straight year, the Philippines failed to enact new counterterrorism legislation. Lawmakers introduced several counterterrorism bills in the new Congress in July 2004; however, the executive branch has yet to develop a strategy to identify the most effective legislation or complete the draft of its version and mobilize resources to lobby for its passage. In lieu of specific counterterrorist legislation, the government has broadly criminalized terrorist financing through Republic Law legislation, which defines "hijacking and other violations under Republic Act No. 6235; destructive arson and murder, as defined under the Revised Penal Code, as amended, included those

perpetrated by terrorists against non-combatant persons and similar targets" as one of the violations under the definition of unlawful acts. The Revised Implementing Rules and Regulations R.A. No. 9160, as amended by R.A. No.9194 further state that any proceeds, derived or realized from an unlawful activity includes all material and monetary effects will be deemed a violation against the law.

The Government of the Republic of the Philippines has made impressive progress enhancing and implementing its amended anti-money laundering legislation. It should continue to focus on effective implementation of the laws and procedures already enacted, in part by expanding its financial and human resources to properly equip and train law enforcement and regulatory personnel. Finally, Philippines should enact and implement new legislation that criminalizes terrorism and terrorist financing.

## **Poland**

Poland's geographic location places it directly along one of the main routes between the former Soviet Union republics and Western Europe used by narcotics-traffickers and organized crime groups. According to Polish government estimates, narcotics-trafficking, organized crime activity, auto theft, smuggling, extortion, counterfeiting, burglary, and other crimes generate criminal proceeds in the range of \$2-3 billion yearly. The Government of Poland (GOP) estimates the unregistered or gray economy, used primarily for tax evasion, may be as high as 15 percent of Poland's \$230 billion GDP; it believes the black economy is only one percent of GDP. Poland's entry into the European Union (EU) in May 2004 increased its ability to control its eastern borders, thereby allowing Poland to become more effective in its efforts to combat all types of crime, including narcotics-trafficking and organized crime.

Poland's banks serve as transit points for the transfer of criminal proceeds. As of December 2004, 60 commercial banks were licensed for operation in Poland, as were slightly less than 600 "cooperative banks" that serve the rural and agricultural community. The GOP considers the nation's banks, insurance companies, and brokerage houses to be important venues of money laundering. Polish casinos may likewise be sites for money laundering activity. According to the GOP, fuel smuggling, during which local companies and organized crime groups seek to avoid excise taxes by forging gasoline delivery documents, is a major source of proceeds to be laundered. It is also believed that some money laundering in Poland derives from Russia and/or other countries of the former Soviet Union.

The Criminal Code criminalizes money laundering. Article 299 of the Criminal Code addresses self-laundering and criminalizes tipping off. In June 2001, the parliament passed amendments that broadened the definition of money laundering to encompass all serious crimes ("Act on Counteracting Introduction into Financial Circulation of Property Values Derived from Illegal or Undisclosed Sources," known as the "Act of 16 November"). In March 2003, Parliament further amended the law to broaden the definition of money laundering to include assets originating from illegal or undisclosed sources.

The National Security Strategy of Poland has labeled the anti-money laundering effort as a top priority. The GOP has worked diligently to bring its laws into full conformity with EU obligations. On November 16, 2000, a law went into effect that improves Poland's ability to combat money laundering (entitled "the November 2000 Act on Counteracting Introduction into Financial Circulation of Property Values Derived from Illegal or Undisclosed Sources"). The GOP has updated this law several times to bring it into conformity with EU standards and to improve its operational effectiveness. This law increases penalties for money laundering and contains safe harbor provisions that exempt financial institution employees from normal restrictions on the disclosure of confidential banking information. The law also provides for the creation of a Financial Intelligence Unit (FIU), the General Inspectorate of Financial Information (GIIF), housed within the Ministry of Finance, to collect and analyze large and suspicious transactions.

A major weakness of Poland's initial money laundering regime was that it did not cover many non-bank financial institutions that had traditionally been used for money laundering. To remedy this situation, between 2002 and 2004, the Parliament passed several amendments to the 2000 money laundering law. The amendments expand the scope of institutions subject to identity verification, record keeping, and suspicious transaction reporting requirements. Financial institutions subject to the

reporting requirements prior to March 2004 amendments included banks, the National Depository for Securities, post offices, auction houses, antique shops, brokerages, casinos, insurance companies, investment and pension funds, leasing firms, private currency exchange offices, real estate agencies, and notaries public. The March 2004 amendments to the money laundering law widen the scope of covered institutions to include lawyers, legal counselors, auditors, and charities, as well as the National Bank of Poland in its functions of selling numismatic items, purchasing gold, and exchanging damaged banknotes. It also requires casinos to report the purchase of chips worth 1,000 euros or more. The law's extension to the legal profession was not without controversy. Lawyers strongly opposed the new amendments, claiming that the law violates client/attorney confidentiality privileges.

In 2002, Parliament adopted measures to bring the nation's anti-money laundering legislation into compliance with EU standards regarding the reporting threshold, and also amended Poland's customs law to require the reporting of any cross-border movement of more than 10,000 euros in currency or financial instruments. In addition to requiring that the GIIF be notified of all financial deals exceeding 15,000 euros, covered institutions are also required to file reports of suspicious transactions, regardless of the size of the transaction. Polish law also requires financial institutions to put internal anti-money laundering procedures into effect—a process that is overseen by the GIIF.

The GIIF began operations on January 1, 2001. In its first year of existence, the GIIF received over 350 suspicious transaction reports (STRs). In 2002, the GIIF received 670 STRs, from which prosecutors prepared 70 cases. In 2003, the GIIF received 965 STRs, resulting in the development of 152 cases by the Prosecutor's Office. Between January and November 2004, the GIIF received 1,240 STRs, resulting in the creation of 136 cases. Banks filed eighty percent of the STRs submitted in 2004. At a minimum, all reports submitted by the GIIF to the Prosecutor's Office have resulted in the instigation of initial investigative proceedings. Although there were only four convictions under the money laundering law in 2004 (this figure is twice the number from 2003), many of the investigations begun by the GIIF have resulted in convictions for other non-financial offenses. As of December 2004, the GIIF received 7.5 million reports on transactions exceeding the threshold level. The GIIF receives approximately 1.5 million reports per month.

The vast majority of required notifications to the GIIF are sent through a newly developed electronic reporting system, which is Europe's most technically sophisticated and collects more complete information than the previously required report regarding the transaction in question (e.g., how payment was made—cash or credit, where and when). Only a small percentage of notifications are now submitted by paper, mainly from small institutions, which lack the IT capacity to use the electronic system. Although the new system is an important advance for Poland's anti-money laundering program, the processing and analyzing of the large number of reports that are sent to the GIIF will prove to be a challenge for the understaffed FIU. To help improve the FIU's efficiency in handling the large volume of reports filed by obliged institutions, the GIIF plans to install new analytical software that will permit advanced and detailed analysis of financial information.

The GIIF also does on-site training and compliance monitoring investigations. In 2004, the GIIF carried out 15 compliance investigations and received several hundred follow-up reports from institutions responsible for routinely supervising covered institutions. In January 2004, the GIIF introduced a new electronic learning course designed to familiarize obliged institutions with Poland's anti-money laundering regulations.

The Polish Code of Criminal Procedure, Article 237, allows for certain Special Investigative Measures. However, money laundering investigations are not specifically covered, although the organized crime provisions might apply in some cases. Two main police units deal with the detection and prevention of money laundering: the General Investigative Bureau and the Unit for Combating Financial Crime. Overall, both police units cooperate well with the GIIF. The Internal Security Agency (ABW) may also investigate the most serious money laundering cases.

A recognized need exists for an improved level of coordination and information exchange between the GIIF and law enforcement entities, especially with regard to the suspicious transaction information that the GIIF forwards to the National Prosecutor's Office. To alleviate this problem the GIIF and the National Prosecutor's Office signed a "cooperation agreement" in 2004. The agreement calls for the

creation of a computer-based system that would facilitate information exchange between the two institutions. Work on the development of this new system is currently underway.

The GIIF is authorized to put a suspicious transaction on hold for 48 hours. The Public Prosecutor then has the right to suspend the transaction for an additional three months, pending a court decision. In 2004, Article 45 of the criminal code was amended to further improve the government's ability to seize assets. On the basis of the amended article, an alleged perpetrator must prove that his assets have a legal source; otherwise, the assets are presumed to be related to the crime and as such can be seized. Both the Ministry of Justice and the GIIF desire to see more aggressive asset forfeiture regulations. However, because the former communist regime employed harsh asset forfeiture techniques against political opponents, lingering political sensitivities make it difficult to approve stringent asset seizure laws. In 2003, the GIIF suspended 20 transactions worth 9 million euros and blocked 9 accounts worth 5.2 million euros. During the first eleven months of 2004, the GIIF suspended 5 transactions worth 650,000 euros and blocked 12 accounts worth 2.1 million euros.

The GOP recently created an office of counterterrorist operations within the National Police. The office coordinates and supervises regional counterterrorism units and trains local police in counterterrorism measures. Poland has also created a terrorist "watch list" of entities suspected of involvement in terrorist financing. The list contains data based on information derived from similar lists published by the UN, the EU, and the United States Treasury Department. All covered institutions are required to verify that their customers are not included on the watch list. In the event that a covered institution discovers a possible terrorist link, the GIIF has the right to suspend suspicious transactions and accounts. Despite these efforts, Poland has not yet criminalized terrorist financing, arguing that all possible terrorist activities are already illegal and serve as predicate offenses for money laundering and terrorist financing investigations. The Ministry of Justice has completed draft amendments to the criminal code that would criminalize terrorist financing as well as elements of all terrorism-related activity. The amendments have been presented to the Minister of Justice, but have not yet been approved by Parliament.

Poland is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism, the European Convention on Extradition and its Protocols, the European Convention on Mutual Legal Assistance in Criminal Matters, and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. In November 2001, Poland ratified the UN Convention against Transnational Organized Crime, which was in fact a Polish initiative.

As a member of the Council of Europe, Poland participates in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) and has undergone first and second round mutual evaluations by that group. The GIIF is an active participant in the Egmont Group and in FIU.NET, the EU-sponsored information exchange network for FIUs. Poland has expressed an interest in joining the Financial Action Task Force (FATF).

A Mutual Legal Assistance Treaty between the United States and Poland came into force in 1999. In addition, Poland has signed bilateral mutual legal assistance treaties with Sweden, Finland, Ukraine, Lithuania, Latvia, Estonia, Germany, Greece, and Hungary. Polish law requires the GIIF to have memoranda of understanding (MOUs) with other international competent authorities before it can participate in information exchanges. The GIIF has been diligent in executing MOUs with its counterparts in other countries, signing a total of 20 MOUs between 2002 and 2003. The GIIF-FinCEN MOU was signed in fall 2003. An additional seven memoranda on exchange of financial information with Andorra, Cyprus, Monaco, Germany, Portugal, Thailand, and Ukraine were signed in 2004. Because Poland is an EU member state, the exchange of information between the GIIF and the FIUs of other member states is regulated by the EU Council Decision of October 17, 2000. All information exchanged between the GIIF and its counterparts in other EU states takes place via FIU.NET. For the first eleven months of 2004, 40 requests regarding 124 entities were received by the GIIF from foreign authorities. During the same time period, the GIIF made 104 requests regarding 227 entities to foreign authorities.

Over the past several years, the Government of Poland has worked diligently to implement a comprehensive anti-money laundering regime that meets international standards. Further

improvements could be made by promoting additional training at the private sector level and by working to improve communication and coordination between the General Inspectorate of Financial Information and relevant law enforcement agencies. The Code of Criminal Procedure should also be amended to allow the use of Special Investigative Measures in money laundering investigations. This would help to attain a better record of prosecutions and convictions. Poland should also pass specific counterterrorist financing legislation.

## **Portugal**

Portugal is an entry point for narcotics transiting into Europe, and officials of the Government of Portugal (GOP) indicate that most of the money laundered in Portugal is narcotics-related. GOP officials also report that currency exchanges, wire transfers, and real estate purchases are used for laundering criminal proceeds.

Portugal has a comprehensive anti-money laundering regime that criminalizes money laundering and other serious offenses, including terrorism, arms trafficking, kidnapping, and corruption. Act 5/2002 describes specific measures for combating organized and economic crime, particularly with regard to the gathering of evidence in relation to several crimes. All cross-border movements of currency that exceed 12,500 euros must be declared. All financial institutions, including insurance companies, must identify their customers, maintain records for a minimum of ten years, and demand written proof from customers regarding the origin and beneficiary of transactions that exceed 12,500 euros. Non-bank financial institutions, such as casinos, property dealers, lotteries, and dealers in high-value assets, must also identify customers engaging in large transactions, maintain records, and report suspicious transactions to the Office of the Public Prosecutor.

In February 2002, the law governing money laundering (Act 10/2002) was brought into force. This law expands money laundering to include as predicate crimes arms trafficking, extortion, prostitution, trafficking in nuclear materials, trafficking in persons, trafficking in human organs or tissues, child pornography, trafficking in listed species, and tax fraud. Act 10/2002 also extends the list of entities obliged to report large transactions, to include account officers, external auditors, tax consultants, lawyers, solicitors, notaries, registrars, and money carriers. It also includes any other independent entities involved with the purchase and sale of real estate or commercial entities; operations connected with funds, securities, or other assets belonging to clients; opening or management of savings bank accounts or securities accounts; creation, exploitation, or management of companies, trust funds, or similar structures; transfer and buy rights with regard to professional sportsmen and women; and the execution of any financial operation. In addition, the obligated entities have the duty to report any suspicious operation, independent of the transaction amount.

In November 2003, the GOP passed a law revising and tightening the legal framework for foreign currency exchange transactions, including gold, subjecting them to the reporting requirement for transactions exceeding 12,500 euros. Beyond the requirements to report large transactions, foreign exchange bureaus are not subject to any special requirements to report suspicious transactions. The law does, however, give the GOP the authority to investigate suspicious transactions without notifying targets of the investigation.

On March 27, 2004, Portugal implemented the European Union's (EU) Second Money Laundering Directive through a new law, Act No. 11/2004 Establishing the Regime for Prevention and Repression of the Laundering of Benefits of Illicit Origin. The new law expands police access to information about bank accounts and financial transactions of individuals or companies under investigation. These rules also apply to bank branches outside of Portugal. Under the new rules, which supersede previous legislation, if a bank suspects or knows about a suspicious or illegal transaction, or has concerns about the amount, means, or payment used in the transaction, or any other suspicious fact, the bank must inform the Attorney General's Office. The Attorney General may order the bank not to complete the transaction. If stopping the transaction is impossible or likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering operation, the Attorney General also may allow the bank to proceed with the transaction but require it to provide complete details to the government. Another provision requires banks to provide full access to investigators with a judicial warrant. Until March 2004, banking secrecy laws made it extremely difficult for investigators to obtain information about bank accounts and financial transactions of individuals or companies without their permission.

In addition, new rules, which take effect January 2005, permit tax authorities to lift secrecy rules without authorization from the target of an investigation. The rules require companies to have at least one bank account and, for companies with more than 20 employees, to conduct their business through bank transfers, checks, and direct debits rather than cash. These rules are mainly designed to help the GOP investigate possible cases of tax evasion but may ease enforcement of other financial crimes as well.

Portugal has established regulatory agencies, including the Central Bank of Portugal, the Portuguese Insurance Institution, the Gambling Inspectorate General, the Economic Activities Inspectorate General, the Securities Market Commission, the Registries and Notaries General Directorate, the National Association for Certified Public Accountants and the Association for Assistant Accountants, the Bar Association, and the Chamber of Solicitors, to monitor and enforce the reporting requirements of the obliged entities.

Suspicious transaction reports (STRs) are forwarded for analysis to the Unidade de Informação Financeira (UIF), formerly the Central Unit for Money Laundering Investigation, which began operating as the Financial Intelligence Unit (FIU) for Portugal in June 2003. If money laundering is indicated, the Portuguese Judicial Police will conduct an investigation. The UIF received 251 STRs in 2001, 256 STRs in 2002, and 488 STRs in 2003 from banks and other financial entities.

The Portuguese Madeira Islands International Business Center (MIBC) has a free trade zone, an international shipping register, offshore banking, trusts, holding companies, stock corporations, and private limited companies. The latter two business groups, of which there are approximately 6,500 companies registered in Madeira, are similar to international business corporations. All entities established in the MIBC will remain tax exempt until 2011. Twenty-seven offshore banks are currently licensed to operate within the MIBC. The Madeira Development Company supervises offshore banks.

Companies can also take advantage of Portugal's double taxation agreements. Decree-Law 10/94 permits existing banks and insurance companies to establish offshore branches. Applications are submitted to the Central Bank of Portugal for notification, in the case of EU institutions, or authorization, in the case of non-EU or new entities. The law allows establishment of "external branches" that conduct operations exclusively with nonresidents or other Madeiran offshore entities, and "international branches" that conduct both offshore and domestic business. Although Madeira has some local autonomy, Portuguese and EU legislative rules regulate its offshore sector, and the competent oversight authorities supervise it. Exchange of information agreements contained in double taxation treaties allow for the disclosure of information relating to narcotics or weapons trafficking. Bearer shares are not permitted.

Portuguese laws provide for the confiscation of property and assets connected to money laundering, and authorize the Judicial Police to trace illicitly obtained assets (including those passing through casinos and lotteries), even if the predicate crime is committed outside of Portugal. Police may request files of individuals under investigation and, with a court order, can obtain and use audio and videotape as evidence in court. The law allows the Public Prosecutor to request that a lien be placed on the assets of individuals being prosecuted, in order to facilitate asset seizures related to narcotics- and weapons-trafficking, terrorism, and money laundering. Act 10/2002 shifted the burden of proof in cases of criminal asset forfeiture from the government to the defendant; an individual must prove that his assets were not obtained as a result of his illegal activities. The law defines criminal assets as those owned by an individual at the time of indictment and thereafter. The law also presumes that assets transferred by an individual to a third party within the previous five years still belong to the individual in question, unless proven otherwise. GOP law enforcement agencies seized a total of 2.4 million euros in cash and accounts in 2003 and 5.1 million euros in 2004 in association with drug and money laundering investigations. Portugal has comprehensive legal procedures that enable it to cooperate with foreign jurisdictions and share seized assets.

In August 2003, Portugal passed Act 52/2003, which specifically defines money laundering and criminalizes the transfer of funds related to the commission of terrorist acts. Portugal has created a Terrorist Financing Task Force that includes the Ministries of Finance and Justice, the Judicial Police, the Security and Intelligence Service, the Bank of Portugal, and the Portuguese Insurance Institution. Portugal has applied all of the Financial Action task Force (FATF) Special Recommendations on



Terrorist Financing. Names of individuals and entities included on the UNSCR 1267 Committee's consolidated list, or that the United States and EU have linked to terrorism, are passed to private sector organizations through the Bank of Portugal, the Stock Exchange Commission, and the Portuguese Insurance Institution. In practice, the actual seizure of assets would only occur once the EU's clearinghouse process agrees to the EU-wide seizure of assets of terrorists and terrorist-linked groups. Portugal is actively cooperating in the search and identification of assets used for terrorist financing. To date, no significant assets have been identified or seized.

Portugal is a member of the Council of Europe, the European Union, and the FATF. Portugal is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. Portugal is a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, and became a party to the UN International Convention for the Suppression of the Financing of Terrorism on October 18, 2002. The Money Laundering Investigation Unit of Portugal's Judicial Police is a member of the Egmont Group.

The Government of Portugal has put into place a comprehensive and effective regime to combat money laundering. Laws passed in 2002 strengthen its ability to investigate and prosecute, and the steps taken in 2003 extend the regime's reach to terrorist financing. Portugal should continue to exercise due diligence over its offshore sector and closely monitor domestic non-bank financial institutions.

## **Qatar**

Qatar has a relatively small population (approximately 600,000 residents), with an extremely low rate of general and financial crime. The financial sector, though modern, is limited in size, and subject to strict regulation by the Qatar Central Bank (QCB). There are 15 licensed financial banks, including two Islamic banks and a Qatar Industrial Development Bank. Qatar has 19 exchange houses, three investment companies and one commercial finance company. Although Qatar is a cash-intensive economy, cash placement by money launderers is believed by authorities to be a negligible risk due to the close-knit nature of the society in Qatar and the rigorous "know your customer" procedures required by Qatari law.

On September 11, 2002, the Emir of the State of Qatar signed the Anti-Money Laundering Law. According to Article 28 of the law, money laundering offenses involve the acquisition, holding, disposing of, managing, keeping, exchanging, depositing, investing, transferring, or converting of funds from illegal proceeds. The law imposes penalties of imprisonment of five to seven years, in addition to fines. The law expanded the powers of confiscation of proceeds gained from the commission of a crime, and instrumentalities used to commit a crime, to include the identification and freezing of assets as well as the ultimate confiscation of the illegal proceeds upon conviction of the defendant for money laundering.

The law requires all financial institutions to report suspicious transactions to the QCB and retain records for up to 15 years. The law also gives the QCB greater powers to inspect suspicious bank accounts, and grants the authorities the right to confiscate money in illegal transactions. Article 17 permits Qatar to extradite convicted criminals in accordance with international or bilateral treaties.

The Anti-Money Laundering Law established the National Anti-Money Laundering Committee (NAMLC) to oversee and coordinate money laundering combating efforts. It is chaired by the Deputy Governor of the Qatar Central Bank, in addition to ten other members from the Ministries of Interior, Civil Service Affairs and Housing, Economy and Commerce, Finance, Justice, QCB, Customs and Ports Authority and the State Security Bureau.

In February 2004, passed the Combating Terrorism Law. According to Article Four of the new law, any individual or entity that provides financial or logistical support, as well as raises money for activities considered terrorist crimes according to this statute are to be punished. The punishments are listed in Article Two of the law, which include the death penalty, life imprisonment, and 10 or 15 year jail sentences depending on the crime.

On October 17, 2004 the Government of Qatar appointed a member of the ruling Al-Thani family as director of the Financial Intelligence Unit (FIU). The FIU is responsible for reviewing all financial transaction reports, identifying suspicious transactions and financial activities of concern, ensuring that all government ministries and agencies have procedures and standards to ensure proper oversight of financial transactions, and recommending actions to be taken by the NAMLC if suspicious transactions or financial activities of concern are identified. Qatar's FIU has been active during the new director's appointment. The FIU is coordinating closely with the Doha Securities Market (DSM) to establish procedures and standards to monitor all financial activities that occur in Qatar's stock market. In November 2004, the FIU established monitoring standards in coordination with the National Post Office to ensure that post offices throughout the country monitor carefully all cash transfers. The FIU is also taking steps to monitor financial activities that take place in the Ministry of Justice's Registration Department and Qatar's camel market.

In addition to reporting suspicious transactions, all financial institutions (including businesses conducting hawala transactions) must report transactions Qatari Riyals (QR) 100,000 (approximately \$33,000) or above to the QCB. Any repeated cash transactions of QR 30,000 (approximately \$10,000) or higher made by an individual or entity must be reported. Any transaction of QR 100,000 or higher and repeated transactions of QR 30,000 or higher will be investigated by the FIU in coordination with the Ministries of Justice and Interior. Exchange houses must report any transaction of QR 40,000 or higher. All financial institutions also must identify the person entering into a business relationship or conducting a transaction. In December 2004, QCB installed a central reporting system to assist the FIU in monitoring all financial transactions made by banks.

All accounts must be opened in person. (Only Qatari citizens, legal foreign residents, and citizens of other Gulf Cooperation Council (GCC) states are permitted to open bank accounts.) In January 2002, QCB issued Circular Number 9 regarding the Combat of Money Laundering and Financing of Terrorism. This circular was designed to increase the awareness of all banks operating in Qatar with respect to anti-money laundering efforts, by explaining money laundering schemes and monitoring suspicious activities.

Qatar has taken steps to combat the financing of terrorism, including requiring banks to freeze the assets of the individuals and entities listed on the UN 1267 Sanctions Committee's consolidated list. In 2002, the GOQ established a national committee, to review the consolidated designation lists and to recommend any necessary actions against individuals or entities found in Qatar. On August 24, 2003, the Anti-Money Laundering law was amended (amendment 21/2003) and published in the official gazette. Amendment 21 revised three articles in the anti-money laundering law. Article 2 was amended to broaden the definition for money laundering to include any activities related to terrorist financing. Article 8 added the customs and ports authority to the NAMLC. Article 12 authorized the Central Bank governor to freeze suspicious accounts up to ten days and to inform the attorney general within three days of any action taken. The Attorney General may renew or nullify the freeze order for a period of up to three months. After this process, a freeze order may not be renewed unless authorized by court order.

In March 2004, The Government of Qatar passed a law to establish the Qatar Authority for Charitable Works, which monitors all charitable activity in and outside of Qatar. This law incorporates the Charitable Societies Law (Law No. 8/1998), which outlines the monitoring and supervision of Qatar's charities. The Secretary General of the Authority will approve all international fund transfers by the charities. The Authority will have primary responsibility for monitoring overseas charitable, development, and humanitarian projects that were previously under the oversight of several government agencies such as the Ministry of Foreign Affairs, the Ministry of Finance and the Ministry of Economy and Commerce. Overseas activities must be undertaken in collaboration with a non-governmental organization (NGO) that is legally registered in the receiving country. The Authority will prepare an annual report on the status of all projects and submit the report to relevant ministries. The Authority is in the process of developing concrete measures to exert more control over domestic charity collection.

Article 37 of Law Number 8 of 1998, concerning the establishment and governance of private associations and institutions, stipulates that the Ministry of Awqaf (Endowments) and Islamic Affairs shall oversee and monitor all the activities of private institutions within the boundaries that are

regulated by executive provisions. The Ministry may examine the institution's books, records, and documents that are related to its activities, and it may amend its bylaws. The institution shall provide the Ministry with any information, documents, or other data it requests. According to Article 1 of Law 15 of 1993, banks practicing in offshore business shall be formed either as joint stock companies having their head offices in the State of Qatar or as branches of Qatari or foreign banks.

The QCB, Public Prosecutor and the Criminal Investigation Division (CID) of the Ministry of Interior are the principal entities that have the responsibility for investigating and prosecuting money laundering cases. The FIU receives all suspicious transaction reports and conducts an initial analysis. The FIU also obtains additional information from the banks and other government ministries before determining whether to forward the suspicious report to the Ministry of Interior. The Public Prosecutor and CID work closely on all criminal cases, although in financial cases they often seek the assistance of the QCB. There are no specialized units within the Public Prosecutor or CID's offices that initiate or investigate financial crimes.

Qatar does not yet have any cross-border reporting requirements for financial transactions. Immigration and customs authorities are reviewing this policy and are increasingly interested in expanding their ability to detect trade-based money laundering. The Government of Qatar has established a subcommittee under the NAMLC to implement cross-border reporting requirements. The subcommittee is composed of the QCB, Customs Authority, FIU, and members of the NAMLC. In 2003, the Government of Qatar (GOQ) concluded the investigation of a seizure that occurred in November 2002, involving approximately \$400,000 worth of gold that had been smuggled into the country. The GOQ confiscated all the gold.

Qatar is a party to the 1988 UN Drug Convention but not the UN Convention for the Suppression of the Financing of Terrorism or the UN Convention against Transnational Organized Crime. Qatar 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), a FATF-style regional body that promotes best practices to combat money laundering and terrorist financing in the region. MENAFATF was inaugurated on November 30 in Bahrain by 14 Arab countries. Qatar also participates in the activities of the FATF through its membership in the Gulf Cooperation Council (GCC).

The passage of the Combating Terrorism Law and the establishment of a Financial Intelligence Unit (FIU) demonstrate the Government of Qatar's commitment to fight terrorist financing. Implementation and enforcement of the new law and regulations are essential to the success of Qatar's efforts. Qatar has demonstrated a willingness to work with other countries in the fight against terrorist financing and other financial crimes. Qatar should continue to work to ensure that law enforcement, prosecutors, and customs authorities receive the necessary training and technical assistance to improve their capabilities in recognizing and pursuing various forms of terrorist financing, money laundering and other financial crimes. Qatar should become a party to the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime.

## **Romania**

Romania's geographic location makes it a natural transit country for trafficking in narcotics, arms, stolen vehicles, and persons. As such, the nation is vulnerable to financial crimes. Romania's National Bank estimates the dollar amount of financial crimes to range from \$1 billion to \$1.5 billion per year. Tax evasion and value-added tax (VAT) fraud constitute approximately 45 percent (\$500-\$600 million per year) of this total. Financial sector fraud, fraudulent bankruptcy claims, and smuggling of illicit goods are additional types of financial crimes prevalent in Romania. Romania also has one of the highest occurrences of online credit card fraud in the world.

Laundered money comes primarily from domestic criminal activity carried out by international crime syndicates, which often launder money through limited liability companies set up for this purpose. The U.S. dollar is the preferred currency. Endemic corruption in Romania and its neighboring countries abets money laundering. The proceeds from the smuggling of cigarettes, alcohol, coffee, and other

dutiable commodities are also laundered in Romania. From Romania, most of the laundered funds go to offshore financial shelters in locations such as the U.S. Virgin Islands, Cayman Islands, and Cyprus.

Romania criminalized money laundering with the adoption in January 1999 of Law No. 21/99, On the Prevention and Punishment of Money Laundering. The law became effective in April 1999 and requires customer identification, record keeping, reporting transactions of a suspicious or unusual nature, and currency transaction reporting for transactions over 10,000 euros.

The law also establishes a Financial Intelligence Unit (FIU), known as the National Office for the Prevention and Control of Money Laundering (NOPCML), and mandates that the NOPCML oversee the implementation of internal anti-money laundering procedures and training for all domestic financial institutions covered by the law. The list of entities subject to money laundering controls includes banks, non-bank financial institutions, attorneys, accountants, and notaries. However, in practice, the controls on non-bank financial institutions have not been as rigorous as those imposed on banks.

In December 2002, the Law on the Prevention and Sanctioning of Money Laundering went into effect, changing the list of predicate offenses to the "all-crimes" approach. Every cash operation and every external wire transfer involving a sum exceeding 10,000 euros must be reported to the NOPCML and be monitored. NOPCML is authorized to participate in inspections and controls in conjunction with supervisory authorities.

In addition, the new law expands the number and types of entities required to report to the NOPCML. Some of these new entities include art dealers, travel agents, privatization agents, postal officials, money transferors, and real estate agents. Training for these entities is necessary to ensure compliance with reporting, record keeping, recognition of suspicious transactions, and development of internal controls. The new law also provides for both suspicious transaction reports (STRs) and currency transaction reports (CTR) to be forwarded to the NOPCML, with the CTR amounts conforming to European Union (EU) standards.

In keeping with new international standards, The National Bank of Romania (BNR) introduced Norm No. 3, "Know Your Customer," in December 2003 to strengthen information disclosure for external wire transfers and correspondent banking. When sending out wire transfers, banks must include information about the originator's name, address, and account. The same information is required for incoming wires as well. Banks are further required to undertake proper due diligence before entering into international correspondent relations, and are prohibited from opening correspondent accounts with shell banks. The BNR is currently working on a project to strengthen its anti-money laundering (AML) and counterterrorist financing (CTF) regulations through the introduction of improved bank examination procedures. Plans are also underway to replicate the project in the insurance industry.

The know your customer identification requirements have also been honed, so that identification of the client becomes necessary upon account opening and when single or multiple transactions meet or approach 10,000 euros. In accordance with a new national strategy on money laundering, lawyers are now obligated to report to the NOPCML. In addition, and in line with the Second EU Directive, tipping off has been prohibited. Romanian law permits the disclosure of client and ownership information to bank supervisors and law enforcement authorities, and protects banking officials with respect to their cooperation with law enforcement.

In June 2004, the Government of Romania (GOR) appointed a new director to head the NOPCML. As a result of this new appointment, there has been a concerted effort to increase the NOPCML's operational efficiency and to bring greater visibility to the importance of AML and CTF efforts in Romania. To date, some of the most significant improvements made include the approval of a new organizational structure for the FIU (as mandated by Governmental Decision No. 1078/2004), as well as the passage of legislation that is designed to improve the procedures for analyzing STR information and the suspension of suspicious accounts and transactions.

Thus far, it appears that these efforts have achieved a degree of success. In the four months following the appointment of the new FIU director, 10 transactions amounting to approximately \$1.5 million were suspended (during the last five years, only five transactions had been suspended). Also, from January 1, 2004 to October 2004, 400 cases have been forwarded to the General Prosecutor's Office, 201 of

which were forwarded after June 2004. Despite these improvements, the NOPCML is still hampered by a lack of sufficient resources (outdated IT systems) and personnel who are in need of comprehensive training regarding AML/CTF issues, as well as training in advanced analytical research methodologies. The Law on the Prevention and Sanctioning of Money Laundering increased the powers of NOPCML, but it did not provide for an increase in administrative capacity. NOPCML has begun a process of international cooperation to exchange information with other FIUs, and has also been working closely with Italy to improve its efficiency and effectiveness through an EU PHARE Project.

In 2003, the number of STRs increased to 882, and during the first three quarters of 2004, 1,241 reports were filed. Out of the 1,241 STRs received by the NOPCML, 1,134 were filed by reporting entities and 107 by the supervisory institutions. The law also provides for feedback to be given, upon request, to NOPCML from the General Prosecutor's Office.

However, efforts to prosecute these cases have been hampered by delays in reporting suspicious transactions, by a lack of resources in some regions, and by insufficient training in conducting complex historical financial investigations. The Directorate of Economic and Financial Crimes of the national police also has a mandate to pursue money laundering. However, despite hundreds of money laundering cases investigated since 2001, the interface with the justice system remains deficient.

Romanian law has some, but limited, provisions for asset forfeiture in the Law on Combating Corruption, No. 78/2000, and the Law on Combating Tax Evasion, No. 87/1994.

On November 24, 2004, the GOR approved a draft amendment to the anti-money laundering law, which is expected to be passed in 2005. The new law provides for a uniform approach to combating and preventing money laundering and terrorist financing. The purpose of the law is to achieve the standard contained in EU Directive 2001/97/EC. The draft law provides that money laundering and terrorist financing will be regulated under the same law to ensure consistent and effective measures against these crimes. The draft recommends the expansion of the types of individuals and institutions which are subject to reporting requirements. These obligations include not only reports on specific suspicious transactions, but also generalized intelligence involving financial patterns and typologies. The new law will also provide for better seizure proceedings, the employment of undercover investigators, and the surveillance of financial accounts and communications.

The GOR announced a national anticorruption plan in early 2003 and passed a law against organized crime in April 2003. A new Criminal Procedure Code was passed and became effective on July 1, 2003. The new Code contains provisions for authorizing wiretapping, intercepting, and recording telephone calls for up to 30 days, in certain circumstances. These circumstances, as provided for within the new Code, include terrorist acts and money laundering.

Romania's political leadership has consistently and unequivocally condemned acts of terrorism. After the events of September 11, 2001, Romania passed a number of legislative measures designed to sanction acts contributing to terrorism. Emergency Ordinance 141, passed in October 2001, legislates that the taking of measures, or the production or acquisition of means or instruments with an intention to commit terrorist acts, are offenses of exactly the same level as terrorist acts themselves. These offenses are punishable with imprisonment ranging from five to 20 years.

In April 2002, the GOR's Supreme Defense Council of the Country (CSAT) adopted a National Security Strategy, which includes a General Protocol on the Organization and Functioning of the National System on Preventing and Combating of Terrorist Acts. This system, effective July 2002 and coordinated through the Intelligence Service, brings together and coordinates a multitude of agencies, including 14 ministries, the General Prosecutor Office, the National Bank, and the NOPCML. The GOR has also set up an inter-ministerial committee to investigate the potential use of the Romanian financial system by terrorist organizations.

The Romanian Government and the BNR in particular have been fully cooperative in seeking to identify and freeze terrorist assets. Emergency Ordinance 159, also passed in 2001, includes provisions for preventing the use of the financial and banking system to finance terrorist attacks, and sets forth the parameters for the government to combat such use. The BNR, which oversees all

banking operations in the country, also issued Norm No. 5 in support of Emergency Ordinance 159. Emergency Ordinance 153 was passed to strengthen the government's ability to carry out the obligations under UNSCR 1373, including the identification, freezing, and seizure of terrorist funds or assets.

In November 2004, the Parliament adopted law 535/2004 on preventing and combating terrorism, which abrogates some of the previous government ordinances and takes over most of their provisions. The law includes a chapter on combating the financing of terrorism by prohibiting financial and banking transactions with persons included on international terrorist lists, and requiring authorization for transactions conducted with entities suspected of terrorist activities in Romania.

The BNR receives lists of individuals and terrorist organizations from the United States, the UNSCR 1267 Sanctions Committee, and the EU, and circulates these to banks and financial institutions. The new law on terrorism provides that the assets used or provided to terrorist entities will be forfeited, together with finances resulting from terrorist activity. To date, in regard to terrorist financing, no arrests, seizures, or prosecutions have been carried out.

The EU's Europe Agreement with Romania provides for cooperation in the fight against drug abuse and money laundering. Romania is a member of the Council of Europe (COE) and participates in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). A mutual evaluation in April 1999 by that Committee uncovered a number of areas of concern, including the high evidence standard required for reporting suspicious transactions, a potential conflict with the bank secrecy legislation, and the lack of provisions for cases in which the reporting provisions are intentionally ignored. Romania has been working to address these concerns, bringing in legal experts from the EU to consult. In late 2003, Romania also underwent a Financial Sector Assessment Program (FSAP) by the World Bank as part of that organization's pilot program.

The GOR recognizes the link between organized crime and terrorism. Bucharest is the site of the Southeast European Cooperative Initiative's Center for Combating Transborder Crime, a regional center that focuses on intelligence sharing related to criminal activities, including terrorism. Romania also participates in a number of regional initiatives to combat terrorism. Romania has worked within SEEGROUP (a working body of the NATO initiative for Southeast Europe) to coordinate counterterrorist measures undertaken by the states of Southeastern Europe. The Romanian and Bulgarian interior ministers signed an inter-governmental agreement in July 2002 to cooperate in the fight against organized crime, drug smuggling, and terrorism.

The NOPCML is a member of the Egmont Group. The Mutual Legal Assistance Treaty signed in 2001 between the United States and Romania entered into force in October 2001. The GOR has demonstrated its commitment to international anticrime initiatives by participating in regional and global anticrime efforts. Romania is a party to the 1988 UN Drug Convention, the Agreement on Cooperation to Prevent and Combat Transborder Crime, and the UN Convention against Transnational Organized Crime. Romania also is a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime; the Council of Europe's Criminal Law Convention on Corruption; and the UN International Convention for the Suppression of the Financing of Terrorism. On November 2, 2004, Romania became a party to the UN Convention against Corruption.

Although legislation and regulations designed to combat financial crime are fairly new developments, they are quite comprehensive in scope. Nevertheless, implementation lags, while reporting and investigations are not as timely or as effective as desired. The Government of Romania should continue addressing the concerns of the Council of Europe evaluators by making further improvements in its anti-money laundering regime. Romania should ensure non-bank entities are fully aware of their reporting and record keeping responsibilities and are adequately supervised. Romania should adopt procedures for the timely freezing, seizure, and forfeiture of criminal- or terrorist-related assets. Romania should adopt reporting requirements for the cross-border movement of currency and monetary instruments.

## **Russia**

Russia has enjoyed rapid economic growth in recent years, mainly driven by high world oil prices and the pursuit of sound fiscal policies. Yet, Russia has been slow to complete structural reforms of the banking sector, and overall public confidence in Russian banks remains low. Consequently, Russia's financial system is unattractive to both legal and illegal depositors, and therefore Russia is not considered an important regional financial center. Over the past three years, however, Russia has committed significant resources to improve its ability to combat the laundering of criminal financial proceeds domestically and internationally. Through aggressive enactment and implementation of comprehensive money laundering and counterterrorism financing legislation, Russia now has well-established legal and enforcement frameworks to deal with money laundering and terrorism financing.

Despite notable progress and demonstrated political will to combat these phenomena aggressively, Russia remains vulnerable to criminal financial activity because of a number of contributing factors, namely: vast natural resource wealth, pervasiveness of organized crime, and a high level of corruption. Other factors include porous borders, Russia's role as a geographic gateway to Europe and Asia, a weak banking system, and under-funding of regulatory and law enforcement agencies. Criminal elements from Russia and neighboring countries continue to use Russia's financial system to launder money, because of familiarity with the language, culture, and economic system. The majority of the funds do not appear to be from activities related to narcotics production or trafficking, although these activities likely occur. Experts believe that most of the dirty money flowing through Russia derives from domestic criminal or quasi-criminal activity, including evasion of tax and customs duties and smuggling operations.

Net flows of money out of the country have slowed noticeably since the 1998 financial crisis. Although net capital outflows for the first three quarters of 2004 totaled \$10.9 billion, compared with \$3.8 billion in 2003, the long-term trend in outflows continues to drift downward. This year's anomalous increase was largely attributed to instability in the banking sector and uncertainties in the investment climate. The majority of these outflows involve legitimate movement of money to more secure and profitable destinations abroad, but at least a portion of this money undoubtedly involves the proceeds of criminal activity.

Russia has the legislative and regulatory framework in place to pursue and prosecute financial crimes, including money laundering and terrorism finance. The Russian Federation's (RF's) Federal Law No. 115-FZ "On Combating Legalization (Laundering) of Criminally Gained Income and Financing of Terrorism" became effective on February 1, 2002, with subsequent amendments to the laws on banking, the securities markets, and the criminal code taking effect in October 2002, January 2003, and December 2003. RF 115-FZ obligates banking and non-banking financial institutions to monitor and report certain types of transactions, keep records, and identify their customers. Article 8 of Law 115-FZ provides for the establishment of Russia's financial intelligence unit as an independent executive agency administratively subordinated to the Ministry of Finance. In March 2004, President Putin issued a decree to upgrade the unit, formerly called the Financial Monitoring Committee, to a service, now called the Federal Service for Financial Monitoring (FSFM). All financial institutions with an obligation to report certain transactions must send this information to the FSFM. The FSFM is also responsible for coordinating all of Russia's anti-money laundering and counterterrorism financing efforts, but has no law enforcement investigative powers.

Consistent with Financial Action Task Force (FATF) recommendations, the criminal code was amended in December 2003 to remove a specific monetary threshold for crimes connected with money laundering, thus paving the way for prosecution of criminal offenses regardless of the sum involved.

According to the original language of RF 115-FZ, those institutions legally required to report included: banks, credit organizations, securities market professionals, insurance and leasing companies, federal postal service, jewelry and precious metals merchants, betting shops, and companies managing investment and non-state pension funds. Amendments to the law that came into force on August 31, 2004, extend the reporting duty to real estate agents, lawyers and notaries, and persons rendering legal/accountancy services that involve certain transactions (e.g., preparing/executing transactions with immovables; managing money, securities, or other property; managing bank accounts or securities accounts; attracting or managing money for organizations; or incorporating, managing, and buying/selling organizations).

Various regulatory bodies ensure compliance with Russia's anti-money laundering and counterterrorism finance laws. The FSFM is specifically responsible for regulating leasing companies, pawnshops, and gambling services. The CBR supervises credit institutions; the Ministry of Finance oversees insurance companies, entities managing non-government pension and investment funds, and entities buying and selling precious metals or stones; the Federal Service for Financial Markets supervises professional participants in the securities sector.

The CBR has issued guidelines regarding anti-money laundering practices within credit institutions, including "know your customer" (KYC) and bank due diligence programs. Banks are required to obtain and retain for five years information regarding individuals and legal entities and beneficial owners of corporate entities. Further, banks must adopt internal compliance rules and procedures and appoint compliance officers. In July 2004, Russia amended Law 115-FZ to require banks to identify the original source of funds and to report to the FSFM all suspicious transactions, as opposed to only transactions containing certain features, as previously mandated. Institutions that fail to meet mandatory reporting requirements face revocation of their licenses to carry out relevant activity, limits on certain banking operations, and possible criminal or administrative penalties. An administrative fine of up to \$16,700 can be levied against an institution, with a fine of up to \$700 on an officer of an institution. The maximum criminal penalty is 10 years in prison with applicable fines.

The CBR instituted a number of regulatory measures in 1999 to scrutinize offshore financial transactions. In the six months following the implementation of these regulations, wire transfers from Russian banks to offshore financial centers dropped significantly. At the same time the CBR curtailed establishing correspondent relations with offshore banks by raising the standards for "eligible" offshore financial institutions, thereby reducing their number. In August 2003 the CBR issued Order 1317-U, which regulates the relations of Russian financial institutions with their counterparts in offshore zones. In addition to requiring Russian financial institutions to report all related transactions, offshore banks are in some cases subject to enhanced due diligence and maintenance of additional mandatory reserves to offset potential risks undertaken by the Russian institution for specific transactions.

Foreign financial entities, including those from known offshore havens, are not permitted to operate directly in Russia: they must do so solely through subsidiaries incorporated in Russia, which are subject to domestic supervisory authorities. During the process of incorporating and licensing these subsidiaries, Russian authorities must identify and investigate each director of the Russian unit; therefore nominee or anonymous directors are, as a practical matter, not permitted under Russian law and regulation. As the CBR completes its review of banks' applications for admission into the newly created Deposit Insurance System, the CBR will verify that banks are carrying out these identification procedures before approving the application.

Russian businesses must obtain government permission before opening operations abroad, including in offshore zones. A department within the Ministry of Economic Development and Trade (MEDT) reviews such requests from Russian firms, and once MEDT approves, the CBR must then approve the overseas currency transfer. In either case, the regulatory body responsible for the offshore activity is the same as for domestic activity, i.e., the Federal Service for Financial Markets regulates brokerage and securities firms, while the CBR regulates banking activity.

All obligated financial institutions must monitor and report to the government: 1) any transaction that equals or exceeds 600,000 rubles (approximately \$20,000) and involves or relates to: cash payments, individuals or legal entities domiciled in states that do not participate in the international fight against money laundering, bank deposits, precious stones and metals, payments under life insurance policies, and/or gambling; 2) all transactions of extremist organizations or individuals included on Russia's domestic list; and 3) suspicious transactions.

Each of the FSFM's seven territorial offices corresponds with one of the federal districts that comprise the Russian Federation. The Central Federal District office is headquartered in Moscow; the remaining six are located in the major financial/industrial regions throughout Russia. The primary functions of the territorial offices are to establish cooperation with regional law enforcement and other authorities to enhance information that comes into the FSFM, and to supervise anti-money laundering and counterterrorism financing legislation compliance by institutions under FSFM supervision. Additionally, the satellite offices must identify and register at the regional level all of the pawnshops, leasing, and



gaming entities under their jurisdiction. They also are charged with coordinating efforts between the Central Bank of Russia (CBR) and other supervisory agencies with respect to implementation of anti-money laundering and counterterrorist financing regimes.

Russia's anti-money laundering law, as amended, provides the FSFM with the appropriate authority to gather information regarding the activities of investment foundations, non-state pension funds, gambling businesses, real estate agents, lawyers and notaries, persons rendering legal/accountancy services, and sales of precious metals and jewelry. Virtually all financial institutions submit reports to the FSFM via encrypted software provided by the FSFM. To date, Russia's national database contains approximately three million reports. The FSFM receives six to seven thousand transaction reports daily. Of these daily reports, approximately 75 percent result from mandatory (currency) transaction reports, and the remaining 25 percent relate to suspicious transactions. Among these, 130 to 150 typically merit further investigation, with 20 to 30 of these cases potentially involving terrorism financing. The FSFM has received approximately 400 reports potentially related to terrorism financing since its inception. Depending on the nature of the activity, the FSFM provides information to the appropriate law enforcement authorities for further investigation, i.e., the Ministry of Internal Affairs (MVD) for criminal matters, the Federal Drug Control Service (FSKN) for narcotics-related activity, or the Federal State Security Service (FSB) for terrorism-related cases.

As part of President Putin's recent administrative reforms, the FSKN now has a full division committed to money laundering, staffed by agents with experience in counternarcotics and economic crimes. This division cooperates closely with the FSFM in pursuing narcotics-related money laundering cases. Over the past year, the FSKN has initiated over 50 such investigations.

With its legislative and enforcement mechanisms in place, Russia has begun to prosecute a number of high-level money laundering cases. As of mid-December 2004, the CBR had revoked the licenses of 28 banks for failure to observe banking regulations. Of these 28, two banks were specifically charged with money laundering—Sodbiznesbank and Novocherkassk City Bank. When the CBR announced on May 13, 2004, that it was revoking the license of Sodbiznesbank because of money laundering charges—the first public announcement of such allegations—it touched off a minor crisis of confidence in the banking system and triggered a depositor run. In October 2004 a series of unconfirmed press articles reported that a Moscow bank was under investigation for financing terrorist acts, including the seizure of the Moscow Theater in 2002. Based on these examples and statistics, Russia has demonstrated a broad-based commitment to enforcing its anti-money laundering and counterterrorism financing legislation and is beginning to see an improvement in compliance levels as a result of its actions.

Russia has a legislative and financial monitoring scheme that facilitates the tracking and seizure of all criminal proceeds. None of this legislation, however, is specifically tied to narcotics proceeds. Russia's laws criminalizing money laundering and terrorist financing also provide for the forfeiture of criminal proceeds. Russian legislation provides for a variety of investigative techniques such as search, seizure, and compelling the production of documents, as well as the identification, freezing, seizing, and confiscation of funds/assets. Where sufficient grounds exist to suppose that property was obtained as the result of a crime, investigators and prosecutors can apply to the court to have the property frozen or seized. Law enforcement agencies have the power to identify and trace property that is, or may become, subject to confiscation or is suspected of being the proceeds of crime or terrorist financing. Moreover, the law allows the FSFM, in concert with banks, to freeze possible terrorist-related financial transactions up to one week. Banks may freeze transactions for two days and the FSFM may follow up with an additional five days.

In accordance with its international agreements, Russia recognizes rulings of foreign courts relating to the confiscation of proceeds from crime within its territory and can fully or partially transfer confiscated proceeds of crime to the foreign state whose court issued the confiscation order. However, Russian law still does not provide for the seizure of instruments of crime. Businesses can be seized only if it can be shown that they were acquired with criminal proceeds. Legitimate businesses cannot be seized solely on the basis that they were used as "instruments" to facilitate the commission of a crime. While Russian law enforcement has adequate police powers to trace and seize assets, most Russian law enforcement personnel lack experience and expertise in these areas.

The Russian Federation has enacted new legislation and executive orders to strengthen its ability to fight terrorism. On January 11, 2002, President Putin signed a decree entitled "On Measures to Implement the UN Security Council Resolution (UNSCR) No. 1373 of September 28, 2001." Noteworthy among this decree's provisions are the introduction of criminal liability for intentionally providing or collecting assets for terrorist use, and the instructions to relevant agencies to seize assets of terrorist groups. This latter clause, however, conflicted with existing domestic legislation. Accordingly, on September 24, 2002, the Duma approved an amendment to the anti-money laundering law, resolving the conflict, and allowing banks to freeze assets immediately, pursuant to UNSCR 1373. This law came into force on January 2, 2003. Further, Article 205.1 of the criminal code, which was enacted in October 2002, criminalizes terrorist financing. On October 31, 2002, the Federation Council, Russia's upper house, approved a supplemental article to the 2003 federal budget, allocating from surplus government revenues an additional 3 billion rubles (\$100 million) in support of federal counterterrorism programs and improvement of national security.

In February 2003, at the request of the General Procuracy, the Russian Supreme Court issued an official list of 15 terrorist organizations. According to press reports, the financial assets of these organizations were immediately frozen. In addition, Russia has assisted the United States in investigation of terrorist financing, providing vital financial documentation and other evidence establishing the criminal activities of the Benevolence International Foundation (BIF). Russian authorities have also provided U.S. federal law enforcement authorities with valuable evidence relating to terrorist fundraising activities of an individual currently being prosecuted in the U.S. for possession of counterfeit currency.

Following an aggressive campaign to reform Russia's anti-money laundering regime, Russia became a full FATF member in June 2003. During its first plenary as a full-fledged FATF member, Russia announced its intention to create a Central Asian FATF-style Regional Body (FSRB). In October 2004, Russia successfully kicked off the FSRB, the Eurasian Group on Combating Legalization of Proceeds from Crime and Terrorist Financing (EAG), which includes Belarus, China, Kazakhstan, Kyrgyzstan, Tajikistan and Russia as members, and several other nations and multilateral organizations as observers to the group, including the United States. Concurrent with the first plenary meeting of the EAG, Russia also hosted the annual FATF Typologies meeting in Moscow in early December 2004.

The United States and Russia signed a Mutual Legal Assistance Treaty in 1999, which entered into force on January 31, 2002. To date, the FSFM has signed cooperation agreements with the Financial Intelligence Units (FIUs) of the United States, Poland, Britain, the Czech Republic, Belgium, Italy, Panama, France, Estonia, Ukraine, Colombia, Cyprus, Finland, Latvia, Luxembourg, Switzerland, and the United Kingdom. Additionally, the FSFM is an active member of the Egmont Group, having taken on sponsorship of several candidate countries for 2004. U.S. law enforcement agencies exchange operational information with their Russian counterparts on a regular basis.

In addition to membership in the FATF, Russia holds membership in the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL). Russia ratified the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime in January 2001. Russia is a party to the 1988 UN Drug Convention and on May 26, 2004, became a party to the UN Convention against Transnational Organized Crime. In November 2002, Russia ratified the UN International Convention for the Suppression of the Financing of Terrorism. Russia also became a signatory to the UN Convention against Corruption.

Russia has developed a solid legislative and regulatory foundation for combating money laundering and terrorism financing. Given its role in spearheading the creation of the EAG, Russia has demonstrated both the political will and a capability to play a more proactive role in improving the region's capacity for countering money laundering and terrorism financing. Nevertheless, vulnerabilities continue. Russia has committed to improving CBR oversight of shell companies as well as closer scrutiny of banks that do not carry out traditional banking activities. Further, the Government of Russia has drafted a national money laundering strategy, which is currently under review and will likely be enacted in 2005. Finally, endemic and high-level corruption continues to undermine Russia's best efforts. Persistent and significant deficiencies in Russia's overall business operating environment pose formidable challenges to Russia's efforts to establish a well functioning and comprehensive anti-money laundering/counterterrorism financing regime.

The Government of Russia should strive to contain official corruption and increase transparency in the corporate environment. Russia should commit adequate resources to its regulatory and law enforcement entities to enable them to fulfill their responsibilities. Russia should also enact legislation that would provide for the seizure of instruments, as opposed to merely the proceeds, of criminal activity. Finally, Russia should continue to play a leadership role in the region with regard to anti-money laundering and counterterrorist finance regime implementation.

## **Rwanda**

Rwanda is not a major financial center. Since recovering from the 1994 genocide and war, Rwanda's banking system has been largely controlled by the government and is now in the process of privatization. Two of eight banks were privatized in 2004. The Rwandan financial system lacks the efficiencies of more modern banking systems, such as electronic funds transfers or credit card transactions. As that system develops and the country becomes more stable, and as neighboring countries like Kenya and Tanzania increase their enforcement efforts, there is a risk of increased illegal financial activity in Rwanda.

There are no documented reports of money laundering in Rwanda, primarily due to the government's close monitoring through the Central Bank of monetary transfers totaling more than \$50,000, whether domestic or international. The authority for such monitoring is granted in the Rwandan Banking Act of 2000. We do not know if Rwandan financial institutions engage in international narcotics-trafficking transactions or whether Rwanda has entered into bilateral agreements for the exchange of information on money laundering with other countries. Since Rwanda has been the recipient of large amounts of foreign assistance, the IMF and the World Bank continue to monitor the banking sector, particularly with regard to government spending. In addition, most of the country's charitable and nonprofit entities are recipients of international aid and are largely monitored by their donors, the IMF and/or the World Bank.

There is evidence that the Government of Rwanda (GOR) indirectly engaged in mineral transfers from the Congo during the Rwandan occupation of the eastern Congo that ended in the fall of 2002. The National Bank of Rwanda (BNR) and the Rwandan Private Sector Federation (the Rwandan equivalent of the chamber of commerce) both confirmed the large amounts of Rwandan profits obtained from the processing of coltan from 1999 through 2001. According to the BNR, the profits reportedly peaked at \$3 million in customs fees and banking profits in a two-month period in 2000. These profits helped fuel the Rwandan GDP growth rate of 9 percent for 2002. Neither organization could confirm significant transactions in Congolese diamonds.

For the past three years, Rwanda has been completely overhauling its legal system, and the Rwandan Parliament is enacting new legislation affecting Rwandan financial law. There remains no provision for the prosecution of potential money laundering cases, however, and, no regulation of imports and exports, except for post-checks on transferred goods. According to legal experts with the Rwandan Finance Ministry and the Prosecutor General's office, no laws under consideration would curb secrecy in respect to client and ownership information in either domestic or offshore financial transactions. Additionally, there are no laws in place concerning banker negligence or the forfeiture and seizure of assets in cases involving narcotics-trafficking, serious crimes or terrorists. No arrests for money laundering or terrorist financing have occurred in Rwanda since January 1, 2003.

Rwanda has officially committed itself to locating and freezing terrorist assets identified by the international community. However, Rwanda has yet to develop fully its laws and its ability to enforce regulations against terrorist financing in accordance with the relevant UN resolutions. The GOR does, however, retain the power to identify, freeze, and seize terrorist-related financial assets. The Ministry of Finance circulates lists of identified individuals and organizations included on the UNSCR 1267 Sanctions Committee's consolidated list. Rwanda is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism.

The GOR cooperates with the U.S. when requested in connection with investigations and proceedings related to narcotics, terrorism, terrorist financing, and other serious crimes. For example, the Rwandan National Police's (RNP) Economic Crimes Division has cooperated with the USG in check

embezzlement investigations that led to arrests in Uganda. However, the RNP lacks the experience, training, and resources to be effective in investigating and enforcing laws concerning modern money laundering and terrorist financing. Furthermore, no formal body of laws or regulations concerning this cooperation currently exists in Rwanda.

The Government of Rwanda should enact comprehensive anti-money laundering legislation covering all serious crimes, including terrorist financing, and take steps to develop a viable anti-money laundering regime. Rwanda should also consider becoming an observer to the Eastern and Southern Africa Anti-Money Laundering Group.

## **Samoa**

Samoa does not have major organized crime, fraud, or drug problems. The most common crimes that generate revenue within the jurisdiction are primarily the result of low-level fraud and theft. The domestic banking system is very small, and there is relatively little risk of significant money laundering derived from domestic sources. Samoa's offshore banking sector is relatively small. The Government of Samoa (GOS) enacted the Money Laundering Prevention Act (the Act) in 2000. This law criminalizes money laundering associated with numerous crimes, sets measures for the prevention of money laundering and related financial supervision. Newly adopted regulations and guidelines fully implementing this legislation came into force in 2002. Under the Act, a conviction for a money laundering offense is punishable by a fine not to exceed Western Samoa Tala (WST) one million (approximately \$354,000), a term of imprisonment not to exceed seven years, or both.

The Act requires financial institutions to report transactions considered suspicious to the Money Laundering Prevention Authority (MLPA), the Samoa Financial Intelligence Unit (FIU) currently working under the auspices of the Governor of the Central Bank. The MLPA receives and analyzes disclosures, and if it establishes reasonable grounds to suspect that a transaction involves the proceeds of crime, it refers the information to the Attorney General and the Commissioner of Police. In 2003, Samoa established under the authority of the Ministry of the Prime Minister, an independent and permanent Transnational Crime Unit (TCU). The TCU is staffed by personnel from the Samoa Police Service, Immigration Division of the Ministry of the Prime Minister and Division of Customs. The TCU is responsible for intelligence gathering and analysis and investigating transnational crimes, including money laundering, terrorist financing and the smuggling of narcotics and people.

The Act requires financial institutions to record new business transactions exceeding WST 30,000 (approximately \$10,000), to retain records for a minimum of seven years, and to identify all parties to the transactions. This threshold reporting system could expose the financial institutions to potential abuse. Nevertheless, Section 43(a) of the Money Laundering Prevention Regulations 2002 requires financial institutions to identify their customers when "there are reasonable grounds for believing that the one-off transaction is linked to one or more other one-off transactions and the total amount to be paid by or to the applicant for business in respect to all of the linked transactions is WST 30,000, or the equivalent in another currency." Moreover, proposed amendments to the Act would delete the threshold reporting system, leaving it open for all financial institutions to report any amount or transaction that purports to involve money laundering.

Section 12 of the Act establishes that all financial institutions have an obligation under this law to "develop and establish internal policies, procedures and controls to combat money laundering, and develop audit functions in order to evaluate such policies, procedures and controls." The Regulations and Guidelines that have been developed remedy the lack of specificity in the Act about the obligation of financial institutions to establish the identity of the beneficial owner of an account managed by an intermediary. Specifically, Section 12.06 of the Money Laundering Prevention Guidelines for the Financial Sector provides that "...If funds to be deposited or invested are being supplied by or on behalf of a third party, the identity of the third party (i.e., the underlying beneficiary) should also be established and verified." The law requires individuals to report to the MLPA if they are carrying with them WST 10,000 (approximately \$3,300) or more, in cash or negotiable instruments, upon entering or leaving Samoa.

The Act removes secrecy protections and prohibitions on the disclosure of relevant information. Moreover, it provides protection from both civil and criminal liability for disclosures related to potential money laundering offenses to the competent authority.

The Central Bank of Samoa, the Office of the Registrar of International and Foreign Companies, and the MLPA regulate the financial system. There are four locally incorporated commercial banks, supervised by the Central Bank. The Office of the Registrar of International and Foreign Companies has responsibility for regulation and administration of the offshore sector. There are no casinos, but two local lotteries are in operation.

Samoa is an offshore financial center, with eight offshore banks licensed. For entities registered or licensed under the various Offshore Finance Centre Acts, there are no currency or exchange controls or regulations, and no foreign exchange levies payable on foreign currency transactions. No income tax or other duties, nor any other direct or indirect tax or stamp duty is payable by registered/licensed entities. In addition to the eight offshore banks, Samoa currently has 13,465 international business corporations (IBCs), three international insurance companies, six trustee companies, and 175 international trusts. Section 16 of the Offshore Banking Act stipulates prohibition for any person from applying to be a director, manager, or officer of an offshore bank who has been sentenced for an offense involving dishonesty. The prohibition is also reflected in the application forms and Personal Questionnaire that are completed by prospective applicants that detail the licensing requirements for offshore banks. The application forms list the required supporting documentation for proposed directors of a bank. These include references from a lawyer, accountant, and a bank, police clearances, curriculum vitae, certified copies of passports and personal statements of assets and liabilities (if also a beneficial owner). The Inspector of Offshore Banks must be satisfied with all supporting documentation that a proposed director is fit and proper in terms of his integrity, competence and solvency.

International cooperation can occur only if Samoa has entered into a mutual cooperation agreement with the requesting nation. Under the Act, the MLPA has no powers to exchange information with overseas counterparts. All cooperation under the MLPA is through the Attorney General's Office, which is the Competent Authority under the Act for receiving and implementing. However, according to a 2003 Samoa Report to the UN Counter-Terrorism Committee, Samoa is reviewing the legal framework for the effective operation of the MLPA in order to further strengthen domestic and international information exchange. In addition, the Office of the Attorney General, in conjunction with the Central Bank, the Ministry of Police and the Division of Customs of the Ministry for Revenue, is currently preparing amendments to the Money Laundering Prevention Act of 2000 for purposes of strengthening and complementing legislation that is being drafted or developed, including the Proceeds of Crime Bill, the Mutual Assistance in Criminal Matters Bill, and the Extradition Amendment Bill. Samoa is a party to the UN International Convention for the Suppression of the Financing of Terrorism. In 2002, Samoa enacted the Prevention and Suppression of Terrorism Act. The Act defines and criminalizes terrorist offenses, including offenses dealing specifically with the financing of terrorist activities. The combined effect of the Money Laundering Prevention Act of 2000 and the Prevention and Suppression of Terrorism Act of 2002 is to make it an offense for any person to provide assistance to a criminal to obtain, conceal, retain or invest funds or to finance or facilitate the financing of terrorism.

Samoa is a member of the Asia/Pacific Group on Money Laundering and the Pacific Island Forum. Samoa hosted the annual plenary of the Pacific Island Forum in August, 2004. Samoa has not signed the 1988 UN Drug Convention. Nor has it signed the UN Convention against Transnational Organized Crime.

Since the passage of the Money Laundering Prevention Act in June 2000, Samoa has continued to strengthen its anti-money laundering regime and has issued regulations and guidelines to financial institutions so that they have a clear understanding of their obligations under the Act. Particular emphasis is directed toward regulation of the offshore financial sector, principally the establishment of due diligence procedures for owners and directors of banks and the elimination of anonymous accounts for onshore and offshore banks. The GOS is strengthening relevant legislation to identify the beneficial owners of IBCs to help ensure that criminals do not use them for money laundering or other

financial crimes. Samoa is in the process of adopting amended and additional legislation to allow for international cooperation and information sharing.

The inability of the Money Laundering Prevention Authority simply to exchange information on an administrative level is a material weakness of the current system and is an impediment to international cooperation. To rectify that situation, the Government of Samoa should enact legislation to provide the Money Laundering Prevention Authority with the legal authority to share information with foreign analogs. Samoa should also accede to the 1988 UN Drug Convention and become a party to the UN Convention against Transnational Organized Crime.

## **San Marino**

San Marino is a small, landlocked, independent republic located on the eastern side of the Italian peninsula. It is the third smallest country in Europe after the Holy See and Monaco. San Marino was founded in 301 and claims to be the oldest republic in the world. Its policies and social trends closely track those of Italy. The financial sector is a large component of the republic's small economy. The Government of San Marino (GOSM) passed anti-money laundering legislation in 1998. In June 2003 the GOSM approved a law that provides functional integration between the Office of Banking Supervision and the Central Bank, thus strengthening the supervisory system and its efforts to counter money laundering and terrorist financing.

Also in 2003, the Office of Banking Supervision issued Circular No. 33 addressed to banks and financial companies that obligates the collection of customers' personal data and their business/professional activity. The GOSM has also approved a law on the "Provisions of Anti-Terrorism, Anti-Money Laundering and Anti-Insider Trading," which became effective on February 26, 2004. The legislation criminalizes terrorism; introduces rules supplementing the Anti-Money Laundering Law of 1998 by incorporating modifications recommended by the Financial Action Task Force (FATF) and the Council of Europe; provides for the freezing of financial assets or property; allows special investigative techniques; and contains rules on insider trading. In April 2003, San Marino had its second round of mutual evaluations by MONEYVAL.

The GOSM is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. It signed, but has not yet become a party to, the UN Convention against Transnational Organized Crime. The San Marino Financial Intelligence Unit (the Department of Treasury inspection office) will adhere to the Egmont Group at its next meeting in April 2005.

The Government of San Marino should continue its efforts to thwart money laundering and terrorist financing and should ratify the UN Convention against Transnational Organized Crime.

## **Sao Tome and Principe**

Sao Tome, which has a small economy and several commercial banks, is not a regional financial center.

Sao Tome is a party to the 1988 UN Drug Convention but not to the UN International Convention for the Suppression of the Financing of Terrorism or the UN Convention against Transnational Crime. It has not criminalized either money laundering or terrorist financing and has no laws allowing the government to freeze assets related to those activities. The need for it to enact and implement such legislation has been heightened by the successful conclusion of an agreement with Nigeria that will bring substantial oil revenues to the country. Sao Tome should consider devoting a portion of that revenue to develop a comprehensive anti-money laundering/counterterrorist regime that comports with international standards.

The Government of Sao Tome should criminalize money laundering and terrorist financing. Sao Tome should also enact legislation allowing the government to freeze assets related to money laundering and terrorist financing. Sao Tome should become a party to both the UN International Convention for

the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime.

## **Saudi Arabia**

Saudi Arabia is a growing financial center in the Gulf Region of the Middle East. There is little known money laundering in Saudi Arabia related to traditional predicate offenses. All ten commercial banks in Saudi Arabia operate as standard "western-style" financial institutions and all banks operate under the supervision of the Saudi Arabian Monetary Authority (SAMA). Saudi Arabia is not an offshore financial center. There are no free zones for manufacturing, although there are bonded transit areas for the transshipment of goods not entering the country. The money laundering and terrorist financing that does occur are not primarily related to narcotics proceeds in Saudi Arabia. There was no significant increase in financial crimes during 2004, and any market in smuggled goods does not appear to be related to the narcotics trade.

Saudi donors and unregulated charities have been a major source of financing to extremist and terrorist groups over the past 25 years. However, The Final Report of the National Commission on Terrorist Attacks Upon the United States ("The 9/11 Commission") found no evidence that either the Saudi Government, as an institution, or senior Saudi officials individually, funded al-Qaida. Following the al-Qaida bombings in Riyadh on May 12, 2003, the Government of Saudi Arabia has taken significant steps to help counteract terrorist financing.

In 2003, Saudi Arabia approved a new anti-money laundering law that for the first time contains criminal penalties for money laundering and terrorist financing. The law bans conducting commercial or financial transactions with persons or entities using pseudonyms or acting anonymously; requires financial institutions to maintain records of transactions for a minimum of ten years and adopt precautionary measures to uncover and prevent money laundering operations; requires banks and financial institutions to report suspicious transactions; authorizes government prosecutors to investigate money laundering and terrorist financing; and allows for the exchange of information and judicial actions against money laundering operations with countries with which Saudi Arabia has official agreements.

SAMA guidelines correspond to the FATF's Forty Recommendations. On May 27, 2003 SAMA issued updated anti-money laundering and counterterrorist finance guidelines for the Saudi banking system. The guidelines require that banks have mechanisms to monitor all types of "Specially Designated Nationals" as listed by SAMA; that fund transfer systems be capable of detecting specially designated nationals; that SAMA circulars on opening accounts and dealing with charity and donation collection be strictly adhered to; and that the banks be able to provide the remitter's identifying information for all outgoing transfers. The new guidelines also require banks to use software to profile customers to detect unusual transaction patterns; establish a monitoring threshold of SR 100,000; and develop internal control systems and compliance systems. SAMA also issued new "know your customer" guidelines, requiring banks to freeze accounts of customers who do not provide updated account information. Saudi law prohibits non-resident individuals or corporations from opening bank accounts in Saudi Arabia without the specific authorization of the SAMA. There are no bank secrecy laws that prevent financial institutions from reporting client and ownership information to bank supervisors and law enforcement authorities. The Saudi media reported that during 2004, Saudi banks froze more than 250,000 accounts for non-compliance with anti-money laundering and terrorist finance laws. Funds are frozen on the basis of a request submitted from the Minister of Interior or the Minister of Foreign Affairs to the Minister of Finance and National Economy.

The Saudi Arabian Government (SAG) has established an anti-money laundering unit in SAMA and has required Saudi banks to have their own anti-money laundering units with specialized staff to work with SAMA and law enforcement authorities. The SAG has begun to staff a Financial Intelligence Unit (FIU) in the Security and Drug Control Department of the Ministry of the Interior. All banks are also required to report any suspicious transactions to the FIU. When fully operational, the Saudi FIU will collect and analyze suspicious transaction reports and other available information and decide to make referrals the Mabath or other entities for action. It will also coordinate its activities with SAMA's anti-money laundering unit. The FIU will be staffed by officers from the Mabath, SAMA, the Ministry of Commerce, and the Ministry of Interior's Bureau of Investigation and Prosecution. The SAG provides

anti-money laundering training for bank employees, prosecutors, judges, customs officers and other government officials.

Hawala transactions outside banks and licensed moneychangers are illegal in Saudi Arabia. Reportedly, some money laundering cases that SAMA has investigated in the past decade involved the hawala system. In order to help counteract the appeal of hawala, particularly to many of the approximately six million expatriates living in Saudi Arabia, Saudi banks have taken the initiative and created fast, efficient, high quality, and cost-effective fund transfer systems that have proven capable of attracting customers accustomed to using hawalas. An important advantage for the authorities in combating potential money laundering and terrorist financing in this system is that the senders and recipients of fund transfers through this formal financial sector are clearly identified.

Contributions to charities in Saudi Arabia are usually Zakat, which is an Islamic religious duty with specified humanitarian purposes. However, over the past decade, according to a 2002 report to the United Nations Security Council, al-Qaida and other jihadist organizations collected between \$300 and \$500 million and the majority of those funds originated from Saudi charities and private donors. The 9/11 Commission Report noted that the SAG failed to supervise adequately Islamic charities in the country. To help address this problem, in 2002 Saudi Arabia announced its intention to establish a commission to oversee Saudi charities with foreign operations. In 2004, the SAG issued guidelines for the Commission for Relief and Charitable Work Abroad. As required by regulations in effect for over 20 years, domestic charities in Saudi Arabia are licensed, registered, audited, and supervised by the Ministry of Social Affairs. The Ministry, has engaged outside accounting firms to perform annual audits of charities' books and has established an electronic data base for tracking the operations of the charities they oversee. New banking rules implemented in 2003 that apply to charities include stipulations that accounts can be only opened in Saudi Riyals; there are enhanced customer identification requirements; there is one main consolidated account for each charity; there are no cash disbursements—payments may be made only by checks payable to the first beneficiary and deposited in a Saudi bank; the use of ATM and credit cards for charitable purposes will not be permitted; there will be no transfers outside of Saudi Arabia. It is unclear however, whether such regulations, apply to international charities.

Saudi Arabia participates in the activities of the Financial Action Task Force (FATF) through its membership in the Gulf Cooperation Council (GCC). In July 2004, reporting on the results of a mutual evaluation conducted in September 2003, the FATF concluded that the framework of Saudi Arabia's anti-money laundering regime met the general obligations of the FATF recommendations for combating money laundering and financing of terrorism, but noted the need to implement these new laws and regulations.

Saudi Arabia also supported the creation of the Middle East and North Africa Financial Action Task Force (MENAFATF) that was inaugurated in Bahrain in November 2004; the SAG was one of the original charter signatories. The MENAFATF is a FATF-style regional body. The creation of the MENAFATF will be a critical element in the region's efforts to expedite the adoption and implementation of international anti-money laundering and counterterrorist financing standards.

Saudi Arabia is working to implement the UN Security Council Resolutions on terrorist financing. SAMA circulates to all financial institutions under its supervision the UNSCR 1267 Sanctions Committee's consolidated list. In January 2004, Saudi Arabia and the United States made a joint request to the UNSCR 1267 Sanctions Committee to designate the Kenya, Pakistan, Tanzania and Indonesia branches of the al Haramain Islamic Foundation as a supporter of terrorism. In June 2004, Saudi Arabia announced that it had completely dissolved the al Haramain Islamic Foundation. The SAG and U.S. worked bilaterally to investigate terrorist financing. Among other activities, in response to specific requests from the U.S., the SAG investigated financial activities for 41 individuals and found that none had financial activities in the Kingdom.

Saudi Arabia has signed but is not yet a party to the UN International Convention for the Suppression of the Financing of Terrorism. It ratified the UN Convention against Transnational Organized Crime on January 18, 2005.



The Government Saudi Arabia should move rapidly to monitor and enforce the new anti-money laundering and terrorist finance laws, regulations and guidelines. Saudi Arabia can demonstrate its commitment to effective implementation by providing adequate budgets, equipment, and staffing for the FIU and the High Commission for Charities. As in many countries in the region, there is still an over-reliance on suspicious transaction reporting to generate money laundering investigations. Saudi Arabia's unwillingness to publicly disseminate statistics regarding money laundering prosecutions impedes the evaluation and design of enhancements to the judicial aspects of its AML system. Law enforcement agencies should take the initiative and proactively generate leads and investigations, and be able to follow the financial trails wherever they lead. Saudi Arabia should demonstrate its willingness to hold elites accountable. Charities identified with the elites must also be examined and rules enforced. Regarding the misuse of charities, loopholes remain including the ability of a group or individual previously affiliated with suspect charitable organizations to simply cease referring to itself as a charity, as well as with the status of international charities. Donations in the form of gold and other gifts need to be scrutinized. Saudi Arabia should take affirmative steps to close loopholes. It should become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

## **Senegal**

Senegal's banking system and formal and informal money-exchange systems are vulnerable to the laundering of proceeds from corruption, narcotics-trafficking, illegal gems and arms-trafficking, and trafficking in persons, all of which are prevalent in West Africa. A building boom in Dakar despite the relative scarcity of credit suggests that an increasing amount of funds with an uncertain provenance is available for property speculation. Approximately 15 foreign banks, including several French and African banks, have branches in Senegal. Senegal's larger financial institutions function alongside a thriving micro-credit sector and numerous non-traditional financial businesses handling remittances from overseas Senegalese in France, Italy, Spain and the United States. Senegal is not obviously linked to any offshore financial centers. Given the small customer pool, the number of casinos in Senegal (reportedly over 15) is striking.

Article 102 of Senegal's 1997 Drug Code criminalizes narcotics-related money laundering as a misdemeanor punishable by up to 10 years in prison. The Drug Code requires banks to report suspicious transactions believed to be linked to narcotics-trafficking and to keep records between one and ten years, depending on the type of record. The law authorizes the seizure of assets related to narcotics-trafficking. The last money laundering prosecution under this law was in 1999.

In 2000, the Economic Community of West African States (ECOWAS) established the Intergovernmental Action Group against Money Laundering (GIABA), based in Dakar, Senegal. GIABA recently hosted a self-evaluation exercise on anti-money laundering capabilities in conjunction with the International Monetary Fund and ECOWAS member states. A Senegalese magistrate is the acting head of GIABA. The Central Bank of West African States (BCEAO), based in Dakar, is the Central Bank for the countries in the West African Economic and Monetary Union (WAEMU): Benin, Burkina Faso, Guinea-Bissau, Cote d'Ivoire, Mali, Niger, Senegal, and Togo, all of which use the French-backed CFA franc currency, which is also linked to the euro. All bank deposits over approximately \$7,700 made in BCEAO member countries must be reported to the BCEAO, along with customer identification information.

Senegal was the first WAEMU country to pass WAEMU-harmonized legislation establishing a Uniform Law on Money Laundering (the Uniform Law), approved by the National Assembly in October 2003. Previously, criminal prosecution of money laundering had been tied to Senegal's Drug Code. The new legislation makes money laundering/terrorist financing a crime in itself, separate from the criminal origins of the money. Banks and other financial institutions, including charitable and nonprofit entities, are required to know, record and report the identity of customers engaging in significant transactions, meaning those involving at least CFA 5,000,000 (approximately \$10,000). The Uniform Law requires financial institutions to preserve records for at least ten years. Under the provisions of banking regulations, banks and financial institutions must provide, upon request from the BCEAO or Senegal's Banking Commission, any information relating to the list of accounts opened on behalf of suspected launderers, suspected terrorists, and/or suspected terrorist organizations and must notify the BCEAO

of any request or the opening of an account relating to such person or organization. Banking secrecy cannot be invoked to protect suspicious clients.

The Uniform Law also mandates the establishment of a National Office for Financial Information Process (CENTIF), a Financial Intelligence Unit (FIU), that will work with banks and other financial institutions to establish a suspicious transaction reporting system and capacity for evaluating questionable transactions. All financial institutions, businesses, and professionals under the scope of the Uniform Law will be required to report suspicious transactions. Presently, foreign-owned banks in Senegal normally report questionable transactions to their home offices (usually Paris) for vetting. Senegal's FIU will have the legal authority to conduct criminal investigations. The CENTIF will have the authority to share information with other FIUs within the WAEMU as well as with the FIUs of non-WAEMU countries. The Government of Senegal (GOS) has yet to issue a decree directing ministries to second appropriate staff to the CENTIF.

Special units from police forces and "gendarmarie" can be created to investigate and prosecute cases against money laundering. Official statistics regarding the prosecution of financial crimes are unavailable. There have been no arrests and/or prosecutions for money laundering or terrorist financing since January 1, 2004.

The Dakar Industrial Free Trade Zone (ZFD) was established in 1974 to encourage foreign investors to set up intensive export-oriented companies. Its enabling statute has been extended until 2016, but only for companies already established within the zone. The ZFD is largely inactive with few companies present, although a U.S. pharmaceutical company has a manufacturing plant in the ZFD. Police forces and customs officials monitor activities in the free zone. Companies and individuals using the zone are identified and registered.

Terrorism financing is covered in the long-existing "Code Against Acts of Terrorism" which criminalizes the financing of terrorism as required by UNSCR 1373. This provision was incorporated in the Uniform Law. Modifications to the "Code Against Acts of Terrorism" are included in legislation on counterterrorism financing currently under consideration by the National Assembly. The UN 1267 Sanctions Committee consolidated list is circulated both by the GOS and by the BCEAO to commercial financial institutions. To date, no assets relating to terrorist entities have been identified. The WAEMU Council of Ministers issued a directive in September 2002 requesting member countries to pass legislation requiring banks to freeze the accounts of any persons or organizations designated by the UN 1267 Sanctions Committee. A pending law on financing terrorism would meet the stipulations of this directive.

Senegalese authorities acknowledge the existence and use of indigenous alternative remittance systems that bypass, in whole or part, financial institutions. The authorities have established private foreign exchange bureaus to regulate the informal financial sector. No regulation currently governs remittances from the sale of gold and precious stones. There is no requirement to report cross-border currency transactions.

Senegal's Drug Code and Uniform Law include a system to freeze, seize and forfeit narcotics-related assets as well as assets derived from other serious crimes, such as money laundering. It also includes the seizure of instruments of crime such as conveyances used to transport narcotics, or property such as bank accounts, legitimate businesses or real estate. Substitute assets can be seized if relationship to the crime is proven. The Uniform Law allows for both civil and criminal forfeiture, and gives full power and resources to police to trace and seize assets. Financial institutions can freeze assets upon requests from officials from the Ministries of Interior and/or Justice, or from the BCEAO. The Ministry of Justice is responsible for the confiscation of frozen assets. Assets can be frozen for up to 20 years. The sharing of seized narcotics assets with other governments would be the result of case-by-case negotiations.

Senegal has entered into agreements with Tunisia, Morocco and France regarding mutual assistance in criminal matters. With the Uniform Law now in force in most WAEMU countries and with the establishment of GIABA, FIUs in WAEMU and ECOWAS countries will cooperate, exchange and share information. In general, the GOS has demonstrated its commitment and willingness to cooperate with the United States law enforcement agencies, although no formal mechanism exists. In the past

the GOS has worked with INTERPOL and Spanish and Italian authorities on international anticrime operations.

Senegal is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. Senegal also is a signatory to the African Union Convention on Terrorism Finance.

The Government of Senegal should continue to work with its counterparts in the Intergovernmental Action Group against Money Laundering (GIABA) and its partners in WAEMU to establish a comprehensive anti-money laundering regime in the region. Senegal should act timely to make its new Financial Intelligence Unit (FIU) a fully functioning organization, with adequate staffing and resources. Senegal should become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

### **Serbia and Montenegro**

At the crossroads of Europe and on the highway known as the "Balkan route," narcotics-trafficking; smuggling of persons, drugs, weapons and pirated goods; money laundering; and other criminal activities continue in Serbia and Montenegro (SAM, formerly the Federal Republic of Yugoslavia (FRY)). Serbia and Montenegro is located in Southeastern Europe (the Balkans), bordering the Adriatic Sea, between Albania and Bosnia and Herzegovina. SAM is a state union consisting of two republics, the Republic of Serbia and the Republic of Montenegro. In the Republic of Serbia are two nominally autonomous provinces, Kosovo and Vojvodina; a United Nations Administration Mission (UNMIK) has administered Kosovo since 1999. The state union has a population of approximately 10.7 million, of which about 8 million live in Serbia, about 600,000 in Montenegro and slightly over two million in Kosovo. Each republic has a separate government and parliament. However, there is also a parliament on the federal level.

The country has a significant black market for smuggled goods. However, income from narcotics-trafficking is typically not used to support this black market. Rather, it is more typical for drug money to be laundered in the real estate market, which is one of the most popular ways to legalize criminal proceeds in SAM. Tax evasion and trade-based money laundering, in the form of over-and under-invoicing, are also another of the common methods used to launder money. According to government officials, the majority of criminal proceeds from narcotics-trafficking laundered in SAM are derived from illegal activities of the Kosovar "Narco-Mafia." Serbian officials also estimate that up to half of all financial transactions in SAM may be connected in some way to money laundering. Although SAM has made important progress in its fight against corruption and financial crimes by criminalizing money laundering and establishing financial intelligence units, substantial work remains to be done.

Neither republic has identified any activities relating to the financing of terrorism. Montenegro has criminalized the financing of terrorism and Serbia is in the process of amending its criminal code to address this issue.

**State Union.** In March 2002, the leadership of the FRY, Serbia, and Montenegro signed the Belgrade Agreement on restructuring the relationship between the two republics. On February 4, 2003, the FRY parliament voted to adopt a new Constitutional Charter that established the state union of "Serbia and Montenegro." Under this state union structure, most governmental authority previously addressed by federal Yugoslav authorities devolved to the individual republics. As a result, responsibility for the laws and institutions determining policies and legislation has shifted. Consequently, both the Republic of Serbia (Serbia) and the smaller Republic of Montenegro (Montenegro) have addressed money laundering and terrorism financing. However, each republic has done so separately in its own way. Banks in both republics have demonstrated remarkable tolerance for and compliance with the laws in their respective jurisdictions.

In 2001, the federal Yugoslav authorities prepared a national strategy to fight terrorism and established a national coordinating body. However, this body fell into abeyance when the FRY transformed into the state union in February 2003. Ratification of international Conventions and treaties currently lies at the State Union level. All relevant anti-money laundering/counterterrorist financing (AML/CTF) conventions have been ratified.

**Serbia.** The Yugoslav Federal Assembly adopted an Anti-Money Laundering Law (AML Law) in September 2001; it came into effect in July 2002. The AML Law defines money laundering to mean depositing, or introducing into the financial system in any other manner, money which has been acquired through illegal activity. This includes money derived from the gray market economy and from arms and narcotics-trafficking. Criminal penalties for money laundering violations range from six months' to eight years' imprisonment, while civil penalties range from 45,000 to 450,000 dinars (\$650 to \$6,500) per offense.

On July 18, 2003, Serbia passed a new law codifying the powers of the National Bank, decreasing its independence and establishing parliamentary control over its operations. The Bank has adopted AML supervision guidelines and is examining banks for compliance with the existing AML reporting requirements. One area of concern is the large number of currency exchanges located throughout Serbia that are reportedly structuring transactions for clients who want to avoid the reporting requirements. These currency exchanges are regulated by the National Bank, but an effective supervisory scheme to address this problem has not yet been put into place.

Entities subject to reporting requirements include commercial and savings banks and other financial credit institutions, the postal savings bank, the post office, commercial enterprises, all government entities, the National Bank of Yugoslavia and its clearing and payments department, foreign exchange bureaus, casinos, pawnshops, stock exchanges, and national lottery organizers. Covered entities are required to identify persons opening an account or if they are "establishing any other kind of lasting business cooperation with the client," and to report on every cash transaction exceeding 10,000 euros or 600,000 dinars, as well as any suspicious transaction. Similar reporting thresholds apply to insurance policies and cross-border currency transactions. The AML Law also provides for record keeping.

In March 2002, a Financial Intelligence Unit (FIU), the Administration for the Prevention of Money Laundering (FCPML), was established as an independent federal body by governmental decree; it became operational on July 1, 2002. At its founding, both the money laundering law and the FIU were operational at the federal level, with all laws applicable to both Serbia and Montenegro. On February 4, 2003, pursuant to the dissolution of the centralized federal state into the two republic entities, and pursuant to Article 13 of the Constitutional Charter and Implementation Law, the FCPML, up until then a federal FIU, became the FIU for the Serbian Republic. In July 2003, FCPML became a member of the Egmont Group, and has since begun active participation in information exchange with counterpart FIUs.

Despite some positive first steps, the Serbian FIU remains largely ineffective in addressing Serbia's money laundering problems, because of both inadequate funding and a lack of sufficient compliance mechanisms. Other than the memorandum of understanding the FIU signed with the National Bank of Serbia in 2004, the FIU has not formalized relationships with enforcement officials and other government or private institutions for cooperation and exchange of information. For 2003, the FIU reported the receipt of over 60,000 reports and the referral of 162 suspicious cases to law enforcement. However, the FIU has not issued indicators of suspicious activity for all sectors encompassed by the existing law. In addition, the FIU has no inspection authority and has not provided or sponsored adequate training programs for non-bank financial institutions. As a result, the accurate reporting of suspicious transactions is questionable. To cite one example, one of the largest banks in Serbia reported conducting over 15,000 cash transactions in one year. But this same bank had filed less than 10 suspicious transaction reports (STRs) during that same year. Serbia also has not yet obtained a conviction for money laundering.

A new draft money laundering law conforming with international standards, extending the list of covered entities to include attorneys and accountants, and harmonizing legislation with all European Union (EU) Directives, was under review and submitted to Parliament in the beginning of October 2003. The new law was approved by all of the relevant authorities, but then a parliamentary crisis broke out, and the procedure was suspended. On December 28, 2003, Serbia held a parliamentary election that brought to power Prime Minister Kostunica's government. In the last year, however, Kostunica's administration has failed to approve this draft law. To date, the draft law is still in Parliament. Although the draft law is fairly comprehensive, it still has some shortcomings. It does not require suspicious transaction reporting by attorneys (a FATF and EU recommendation), and it does

not establish the FIU as a repository for information relating to the suspicions of terrorist financing, which is now a requirement for all Egmont members.

Serbia has no terrorist financing law consistent with the standards contained in international conventions, and its legislative and institutional framework for combating terrorist financing remains weak. Draft legislation is pending. According to the Serbian Criminal Code, business licenses of legal or natural persons may be revoked and business activities banned if the subject is found guilty of criminal activities, including narcotics-trafficking or terrorist financing. But, despite this fact, Serbia is constrained with regard to international assistance in investigating terrorist financing. This is because Serbia's police may not make use of the Mutual Legal Assistance Treaty (MLAT) process in terrorist financing cases, due to the fact that under Serbian law, use of the MLAT process is restricted to crimes with penal sentences equal to or exceeding ten years (although the draft law reduces the requirement to four years). Under the current law, the maximum term for money laundering or terrorist financing is eight years. As a result, Serbia forfeits any available international assistance. Also presenting another obstacle is Serbia's Criminal Procedure Code, under which an MLAT request for assistance in investigating terrorist activities requires the approval of an investigative judge. However, investigative judges, for a number of reasons, often do not grant these requests. Serbia is currently in the process of amending its Criminal Procedure Code to bring it into conformity with Council of Europe standards. The AML Law establishes special procedures for tracking funds related to terrorist financing. The Serbian FCPML is the authority charged with enforcing the UN terrorism sanction lists. Although it routinely checks for suspect accounts, it has found no evidence of terrorism financing within the banking system and no evidence of the usage of alternative remittance systems. The Department for Combating Organized Crime (UBPOK), in the Ministry of Interior, is the law enforcement body responsible for countering terrorism. UBPOK cooperates and shares information with its counterpart agencies in all of the countries bordering SAM.

Serbia has no asset seizure or forfeiture law. Actual asset seizures can only be carried out by court order.

The government has no encompassing AML/CFT strategy, and has failed to enact anti-money laundering legislation that is in full compliance with international standards. It also has not created a bureaucratic and legal framework that empowers the FIU to carry out its core mission. Terrorist financing laws have not been enacted and the ability to seize or freeze assets relating to terrorist financing, except after a criminal conviction using other statutes, does not exist under current law. As a result of the absence of a comprehensive anti-money laundering regime, no accurate statistical information or feedback regarding cases forwarded to local authorities or prosecutors is available to assess results or ensure transparency. Finally, the Finance Ministry has yet to grant the FIU a line item budget, so that it can effectively plan activities and operations.

**Montenegro.** It is important to note that considering its past record on AML issues, Montenegro has positively and significantly changed its stance on money laundering. In 1996, in an effort to lure needed funds, Montenegro proclaimed itself an offshore area and allowed financial intermediaries to do business-without controls-for a percentage of the profit. Hundreds of millions of dollars worth of money passed through Montenegrin offshore accounts annually. It is speculated that much of the money came from criminal activity.

In August 2002, the Central Bank of Montenegro (CBCG) issued a decree that requires banks and other financial institutions to report suspicious transactions, establish anti-money laundering control programs, and train their employees on money laundering matters. Also, in response to the overwhelming growth of its offshore sector during the past decade, the Montenegrin government mandated that all offshore banks must re-register, post a one million Eurobond or fee, and reestablish themselves as regular banks. To date, since none of the offshore entities has complied with this mandate, the Central Bank has deemed all offshore banks to be dissolved. The Finance Ministry has not released complete information about the actual disposition of the 400 offshore entities whose names they turned over to CBCG.

Money laundering is criminalized in a new Criminal Code, which was amended in June 2003 in order to enable the government to confiscate money and property involved in criminal activity. Additionally, according to the Code, business licenses of legal or natural persons may be revoked and business

activities banned if the subject is found guilty of criminal activities, including narcotics-trafficking or terrorist financing. In April 2004, Montenegro further amended its Criminal Procedure Code to bring it into conformity with the standards of the Council of Europe.

Montenegro passed anti-money laundering legislation on September 24, 2003. The new law obliges banks, post offices, state entities, casinos, lotteries and betting houses, insurance companies, jewelers, travel agencies, auto and boat dealers, and stock exchange entities to file reports on all transactions exceeding 15,000 euros, as well as on any related transactions that aggregate 15,000 euros or more, even if each particular transaction does not exceed the threshold. Financial institutions are also obliged to report suspicious transactions, even if only a small amount of money is involved. Failure to report, according to the law, could result in fines up to 20,000 euros as well as sentences of up to 12 years. The new law establishes mandates for the collection and analysis of these reports by Montenegro's FIU, which also has the responsibility to disseminate these reports to the competent authorities for further action. The FIU is adequately staffed, but compliance mechanisms are as yet untested. The FIU, which has been fully operational since November 2003, is currently a candidate for Egmont membership in 2005.

Montenegro can seize and forfeit assets, but only in connection with a violation of another provision of the Criminal Code, generally money laundering, terrorism or terrorist finance. In September 2004, the Government of Montenegro seized over a million dollars in undeclared currency in connection with the arrest of two Chinese nationals attempting to enter Montenegro.

Amendments to Montenegro's laws on terrorism and terrorist financing were initiated in November 2004 and are expected to be adopted in January 2005. These amendments are designed to bring Montenegrin law into conformance with international standards. Responsibility for the detection and prevention of terrorist financing was transferred in 2004 from the CBCG to the FIU. The FIU promptly informs banks and other financial institutions of additions and changes to the lists of individuals and entities included on the consolidated list of the UNSCR 1267 Sanctions Committee. No terrorist financing has been detected within Montenegro.

**Kosovo.** Since 1999, the United Nations Interim Administration in Kosovo (UNMIK) has governed Kosovo. Therefore, it no longer falls within the jurisdiction of either Serbia or Montenegro. Recognizing that Kosovo could become a haven for money laundering as its neighbors tighten their anti-money laundering regimes, UNMIK determined that Kosovo must also adopt a strict approach to the fight against money laundering. Thus, on February 5, 2004, UNMIK issued Regulation 2004/2, "On the Deterrence of Money Laundering and Related Offenses." The Regulation became effective on March 1, 2004, with delayed effective dates for certain provisions within the regulation.

The Regulation defines the crime of money laundering as the knowing possession, acquisition, use, transfer or conversion of the proceeds of crime. Proceeds of crime is defined as any property derived from any criminal offense punishable by a year or more of imprisonment under the applicable law in Kosovo or under the law of the jurisdiction in which the criminal offense was committed. The crime of money laundering is punishable by up to 10 ten years confinement and a fine up to three times the value of the property laundered. The Regulation provides for both civil and criminal forfeiture of the proceeds of the money laundering or any property which facilitated the money laundering or predicate offense.

The Regulation also obliges banks, non-bank financial institutions (money remitters, securities dealers/brokers, insurance companies, foreign exchange businesses, issuers and sellers of traveler's checks, credit cards, money orders, bank checks, and electronic money), and covered professionals (attorneys, accountants, and licensed auditors) to identify their clients and conduct ongoing due diligence, report suspicious transactions and currency transactions greater than 10,000 euros to the KFIC, maintain records for five years, and maintain an anti-money laundering compliance program which includes the appointment of a compliance officer and mandates training of employees. The Regulation criminalizes tipping off and failure to file either the suspicious transaction report or the currency transaction report. The Regulation also mandates the reporting of the cross-border transportation of monetary instruments exceeding 10,000 euros.

The Regulation creates the Financial Intelligence Centre (KFIC) within the Police and Justice Pillar. The KFIC will receive and analyze the reports received from the various entities, create and maintain a database of all information collected, issue administrative directives, and exchange information upon requests with like foreign entities. The KFIC is functional but in its infancy.

The Regulation limits the receipt by non-governmental organizations (NGOs) of currency contributions to 1000 euros per day from a single source. NGOs cannot distribute greater than 5,000 euros to any single recipient in a single day. NGOs must maintain accounts that document all income and disbursements. The accounts shall identify income by source, amount, and manner of payment, such as currency or payment order, and identify disbursements by recipient, intended use of funds, and manner of payment. NGOs must maintain records for five years, report suspicious transactions to the KFIC and file annual reports.

The Regulation also provides for the widest possible cooperation with foreign jurisdictions with respect to information exchange, investigations and court proceedings in relation to temporary measures for securing property and orders for confiscation relating to instrumentalities of money laundering and proceeds of crime, and for purposes of prosecution of the perpetrators of money laundering and terrorist activity.

SAM has no laws governing its cooperation with other governments, related to narcotics, terrorism, or terrorist financing. Cooperation is instead based on participation in Interpol, bilateral cooperation agreements, and agreements concerning international legal assistance. There are no laws at all governing the sharing of confiscated assets with other countries, nor is any legislation under consideration; SAM may at this time enter into bilateral agreements for this purpose.

Serbia and Montenegro has a legal assistance arrangement with the United States, governed by the 1901 Convention on Extradition of Offenders. SAM has signed 34 bilateral agreements on mutual legal assistance with 26 countries: Albania, Algeria, Austria, Belgium, Bulgaria, the Czech Republic, Denmark, France, Greece, The Netherlands, Croatia, Iraq, Italy, Cyprus, Germany, Poland, Romania, Hungary, Mongolia, Russian Federation, Slovakia, Spain, Switzerland, Turkey, the United Kingdom, and the United States. These agreements authorize extradition of suspected terrorists. Both SAM and its constituent republics cooperate with their counterparts and neighbors. In April 2003, SAM joined eight other participants in the South Eastern Europe Cooperation Process, in adopting a joint "Belgrade Declaration" to call for the continuation of regional cooperation and the intensification of the fight against terrorism and organized crime. SAM worked with Interpol to set up an office for that organization in Belgrade as part of its efforts to contribute to the fight against terrorism and other transnational crimes.

Serbia and Montenegro is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. On October 9, 2003, SAM ratified the Council of Europe's Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. SAM has ratified eight of the 12 UN Conventions or Protocols dealing with terrorism, including the UN International Convention for the Suppression of the Financing of Terrorism, although the domestic implementation procedures do not provide the framework for full application in either republic. In December 2003, SAM signed, but has not yet ratified, the UN Convention against Corruption. As a new member of the Council of Europe, SAM is a full and active member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), and underwent a first-round evaluation by a team from that Committee in October 2003.

Serbia should expand its anti-money laundering legislation to include all serious crimes and to provide for suspicious transaction reporting requirements for intermediaries. Montenegro should enact legislation expanding its anti-money laundering regime, including suspicious transaction reporting requirements, to non-bank financial institutions and intermediaries. Both republics should enact legislation to establish robust asset seizure and forfeiture regimes. Both Serbia and Montenegro should ensure that sufficient resources are available for their FIUs and law enforcement agencies to work effectively and efficiently. Both should also continue to participate in international fora that offer training and technical assistance for police, customs, and judiciary officials involved with combating money laundering and terrorist financing. Serbia should criminalize all aspects of terrorist financing specifically and they should both implement a comprehensive framework to support an

counterterrorism regime that comports with international standards. Kosovo should criminalize terrorist financing and implement its new anti-money laundering law.

## **Seychelles**

Seychelles is not a major financial center, but it does have a developed offshore financial sector, which makes the country vulnerable to money laundering.

The Government of Seychelles (GOS), in efforts to diversify its economy beyond tourism, has taken steps to develop an offshore financial sector to increase foreign exchange earnings. The GOS actively markets Seychelles as an offshore financial and business center that allows the registration of nonresident companies. There are currently over 4,800 registered international business companies (IBCs) in Seychelles that pay no taxes in Seychelles, and are not subject to foreign exchange controls. The Seychelles International Business Authority (SIBA), which acts as the central agency for the registration for IBCs, promotes the fact that IBCs need not file annual reports. The SIBA is part of the Ministry of International Trade, and also manages the Seychelles International Trade Zone.

In addition to IBCs, Seychelles permits offshore trusts (registered through a licensed trustee), offshore insurance companies, and offshore banking. Three offshore insurance companies have been licensed, but no mutual fund companies. The International Corporate Service Providers Act 2003, which is designed to regulate all the activities of the corporate service providers as well as the trustee service providers, entered into force in 2004. A major weakness of the Seychelles' offshore program is that it still permits the issuance of bearer shares, a feature that can facilitate money laundering by making it extremely difficult to identify the beneficial owners of an IBC. Seychelles officials stated in 2000 that they were reviewing the question of bearer shares and intended to outlaw them. In the interim, the GOS has indicated that it will not approve the issuance of any more bearer shares.

No offshore casinos or Internet gaming sites have yet been licensed; if they are, they will be subject to stringent legislation modeled on the Australian Internet Gaming Act. There are no cross-border currency reporting requirements, but the point of entry at Seychelles' international airport is under constant supervision by Customs and the Police, who search suspicious incoming or outgoing passengers.

In 1996, the GOS enacted the Anti-Money Laundering Act (AMLA), which criminalizes the laundering of funds from all serious crimes, requires financial institutions and individuals to report to the Central Bank transactions involving suspected cases of money laundering, and establishes safe harbor protection for individuals and institutions filing such reports. There are no bank secrecy laws in Seychelles. The AMLA imposes record keeping and customer identification requirements for financial institutions, and also provides for the forfeiture of the proceeds of crime.

Under the AMLA, money laundering controls are applied to non-banking financial institutions, including exchange houses, stock brokerages, and insurance agencies, but not to lawyers and accountants. No arrests and/or prosecutions have been made for money laundering and terrorist financing since January 1, 2003.

Under the AMLA, anyone who engages directly or indirectly in a transaction involving money or other property (or who receives, possesses, conceals, disposes of, or brings into Seychelles any money or property) associated with a crime, knowing or having reasonable grounds to know that the money or property is derived from an illegal activity, is guilty of money laundering. In addition, anyone who aids, abets, procures, or conspires with another person to commit the crime, while knowing, or having reasonable grounds for knowing that the money was derived from an illegal activity, is likewise guilty of money laundering.

In 1998, the Central Bank of Seychelles issued a comprehensive set of guidance notes that further elucidated and strengthened the provisions of the AMLA. The Central Bank of the Seychelles receives and analyzes suspicious activity reports and disseminates them to the competent authorities. In November 2002 the Central Bank circulated to all local commercial banks a document on due diligence issued by the Basel Committee.



In December 2004, the Seychelles National Assembly enacted the Financial Institutions Bill 2004, which imposes more stringent rules on banking operations. The Bill, which was drafted in consultation with the International Monetary Fund, aims at ensuring greater transparency in financial transactions and regulating the financial activities of both domestic and offshore banks in line with international standards. One provisions of the new law requires that banks change their auditors every five years. Auditors must notify the Central Bank if they uncover criminal activity such as money laundering in the course of an audit.

In 2004, the GOS enacted the Prevention of Terrorism Bill 2004. The legislation recognizes the government's authority to identify, freeze, and seize terrorist finance-related assets. Currently the Mutual Assistance in Criminal Matters Act of 1995 empowers the Seychelles Central Authority to search and seize anything relevant to a proceeding or investigation relating to a criminal matter involving a serious offense under a written law of a requesting state.

The Prevention of Terrorism Bill strengthens the government's hand in this area. It specifically provides for the forfeiture of assets. Previously, the Seychelles authorities could work only with states that were members of the Commonwealth, or had a treaty for bilateral mutual legal assistance with the Seychelles regarding criminal matters. Under current legislation, assets used in the commission of a terrorist act can be seized, and legitimate businesses can be seized if used to launder drug money, support terrorist activity, or are otherwise related to criminal activities. Both civil and criminal forfeiture are allowed under current legislation. To date, no assets have been identified, frozen, or seized pertaining to terrorist financing, upon request of such a foreign state.

The transactions of charitable and non-profit entities are scrutinized by the authorities to prevent their misuse, and such systems as hawala are regulated.

The Government of Seychelles is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. The Seychelles is a party to the 1988 UN Drug Convention and the UN Convention against Transnational Organized Crime. The Seychelles has signed but not ratified the UN International Convention for the Suppression of the Financing of Terrorism. The Seychelles circulates to relevant authorities the updated lists of designations under Executive Order 13224. Seychelles should expand its anti-money laundering efforts by moving to immobilize bearer shares and requiring complete identification of beneficial owners of international business companies (IBCs). Seychelles should establish a financial intelligence unit to collect, analyze, and share financial data with foreign counterparts, in order to effectively combat money laundering and other financial crimes. Seychelles should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism. Seychelles should criminalize the financing of terrorism and actively participate in ESAAMLG.

## **Sierra Leone**

Sierra Leone, which has a small commercial banking sector, is not a regional financial center. Loose oversight of financial institutions, weak regulations, rampant corruption, and a prevalent informal money-exchange system create an atmosphere conducive to money laundering. Given the importance of the large diamond sector to the economy, the prevalence of money laundering in the diamond sectors of neighboring countries and the loose oversight of the financial sector, Sierra Leone's diamond sector is particularly vulnerable to money laundering. There is no available information for 2004. What follows is a repeat of the 2003.

There is no specific legislation concerning money laundering. However, the Ministry of Justice is in the process of developing such laws. Banks are required to record the identity of customers engaging in large currency transactions and to maintain adequate records necessary to reconstruct significant transactions in order to respond to government information requests. Banks are also required to report suspicious transactions, although they do not usually adhere to this requirement. Bank secrecy laws prevent the disclosure of client and ownership information except under court order.

In 2000, the Economic Community of West African States (ECOWAS) established the Intergovernmental Group for Action Against Money Laundering (GIABA), based in Dakar, Senegal. In

November 2002, GIABA hosted an anti-money laundering seminar for representatives of 14 ECOWAS members, including Sierra Leone.

Sierra Leone is a party to the 1988 UN Drug Convention and has signed, but not yet ratified, the UN Convention against Transnational Organized Crime, which is not yet in force internationally. Sierra Leone has signed, but has not yet become a party to, the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of Sierra Leone should criminalize money laundering and terrorist financing, enforce existing financial laws and regulations, and provide legal authority for the seizure of criminal and terrorist assets.

## **Singapore**

As a significant international financial and investment center, and in particular as a major offshore financial center, Singapore is attractive to potential launderers. Bank secrecy laws and the lack of routine currency reporting requirements make Singapore an attractive destination to foreign drug traffickers, other foreign criminals, and terrorist organizations and their supporters seeking to launder their money, and for flight capital. Money laundering occurs mainly in the offshore sector, but may also occur in the non-bank financial system, which includes large numbers of moneychangers and remittance agencies.

As a leading financial center in Southeast Asia, Singapore has been a key player in the regional effort to stop terrorist financing. Singapore has a sizeable offshore financial sector. In 2004, there were 111 commercial banks in Singapore, of which 47 were offshore banks, down slightly from 50 in December 2003. There are also 23 full banks and 36 wholesale banks in Singapore. All offshore banks are branches of foreign banks. Singapore does not permit shell banks, either in the domestic or offshore sectors. The Monetary Authority of Singapore (MAS), a semi-autonomous entity under the Ministry of Finance, serves as Singapore's Central Bank and financial sector regulator. There are no offshore trusts, although banks may open trust, nominee, and fiduciary accounts. All banks in Singapore, whether domestic or offshore, are subject to the same regulation, record keeping, and reporting requirements, including regarding money laundering and suspicious transactions.

In January 2005, as part of a draft revision of its overall anti-money laundering/counterfinancing of terrorism (AML/CFT) regulations for banks, the MAS proposed, subject to final approval, an amendment to its regulations proscribing banks from entering into, or continuing, correspondent banking relationships with shell banks—in line with the Revised Financial Action Task Force (FATF) Forty Recommendations adopted in June 2003. The new draft regulation also mandates originator information on cross-border wire transfers, in line with the FATF's Special Recommendation Seven on wire transfers. It also clarifies procedures for customer due diligence and includes a risk-based approach to customer due diligence, as well as mandating enhanced customer due diligence for foreign politically exposed persons. It furthermore extends coverage of the regulations to include terrorist financing activities.

Any person who wishes to engage in business, whether local or foreign, must register under the Companies Act. Every Singapore-incorporated company must have at least two directors, one of whom must be a resident in Singapore, and one or more company secretaries, who must be resident in Singapore. There is no nationality requirement. A company incorporated in Singapore has the same status and powers as a natural person. Bearer shares are not permitted. Casinos and Internet gaming sites are currently illegal in Singapore. However, the government is considering lifting the ban on casinos for a specific development project. In December 2004, the Government of Singapore (GOS) invited international investors to submit proposals by February 28, 2005, to build an integrated resort with gambling facilities.

As a matter of policy, Singapore strongly opposes money laundering and terrorist financing. The Corruption, Drug Trafficking, and Other Serious Crimes (Confiscation of Benefits) Act of 1999 (CDSA) criminalizes the laundering of proceeds from narcotics and 183 other serious offenses, including foreign offenses which would be serious offenses if they had been committed in Singapore. Singapore is in the process of reviewing its list of these offenses for consistency with Recommendation 1 of the FATF's Revised 40 Recommendations, and expects to have a final list by June 2005. Financial

institutions must report suspicious transactions and positively identify customers engaging in large currency transactions. Financial institutions are required to maintain adequate records, to be able to respond quickly to GOS inquiries in money laundering cases. However, there are no reporting requirements on amounts of currency brought into or taken out of Singapore. Singapore is considering implementation of FATF Special Recommendation IX, which requires the detection of cross-border movement of currency and bearer negotiable instruments

Banking regulation is the responsibility of the Monetary Authority of Singapore. The MAS performs extensive prudential and regulatory checks on all applicants for banking licenses, including a check to see if the bank is under adequate home country banking supervision. Banks must have clearly identified directors. It is illegal to perform banking transactions without a license.

In 2000, MAS first issued a series of regulatory guidelines ("Notices") requiring banks to apply "know your customer" standards, adopt internal policies for staff compliance, and cooperate with Singapore enforcement agencies on money laundering cases. These Notices are regulatory in nature and are enforceable by prosecution. Similar guidelines exist for securities dealers and other financial service providers. Banks must obtain documentation, such as passports or identity cards, from all personal customers, so that the bank can verify their names, permanent contact addresses, dates of birth, and nationalities, and conduct inquiries into the bona fides of company customers. The regulations specifically require that financial institutions obtain evidence of the identity of the beneficial owners of offshore companies or trusts. The guidelines also mandate specific record keeping and reporting requirements, outline examples of suspicious transactions that should prompt reporting, and establish mandatory intra-company point-of-contact and staff training requirements. Similar guidelines and notices exist for finance companies, merchant banks, life insurers, brokers, securities dealers, investment advisors, and futures brokers and advisors. The MAS announced that it will also revise these Notices in line with the final form of the revised notice for banks.

The Suspicious Transaction Reporting Office (STRO) is Singapore's Financial Intelligence Unit (FIU). Part of the Singapore Police Force's Commercial Affairs Department, it began operating on January 10, 2000. To improve its suspicious transaction reporting, STRO has begun work on a computer system to allow electronic online submission of STRs, as well as the dissemination of AML/CFT material. It plans to encourage all financial institutions and relevant professions to eventually participate in this system.

Singapore is an important participant in the regional effort to stop terrorist financing in Southeast Asia. The Terrorism (Suppression of Financing) Act, passed in 2002, criminalizes terrorist financing, although the provisions of the Act are actually much broader. In addition to making it a criminal offense to deal with terrorist property (including financial assets), the Act criminalizes the provision or collection of any property (including financial assets) with the intention that the property be used, or having reasonable grounds to believe that the property will be used, to commit any terrorist act or for various terrorist purposes.

The Act also provides that any person in Singapore, and every citizen of Singapore outside Singapore, who has information about any transaction or proposed transaction in respect of terrorist property, or who has information that he/she believes might be of material assistance in preventing a terrorism financing offense, must immediately inform the police. The Act gives the authorities the power to freeze and seize terrorist assets. The Act, which supplements and extends interim legislation enacted in November 2001, took effect January 29, 2003.

In January 2003, the Singapore Government released a white paper describing its investigations into the Jemaah Islamiyah (JI) terrorist network. The government is known to have detained 39 persons since 2001 as suspected terrorists. Three persons have been released since then, two in September 2004 and one in January 2005, with restrictions placed on their associations and movements.

In April 2004, the International Monetary Fund and the World Bank Financial Sector Assessment Program (FSAP) team published an assessment of Singapore's financial sector, which included an evaluation of the AML/CFT regime. The IMF found that Singapore's ability to freeze terrorist related funds is comprehensive. The IMF also concluded that, while Singapore has not adopted the FATF approach of designating terrorist financing offenses as predicate crimes for money laundering,

Singapore appears to meet the underlying obligations of the relevant FATF Special Recommendation Two on terrorist financing.

There are few restrictions on intergovernmental terrorist financing-related mutual legal assistance even in the absence of a Mutual Legal Assistance Treaty, because Singapore is a party to the UN International Convention for the Suppression of the Financing of Terrorism, the IMF concluded. But the IMF urged Singapore to improve its mutual legal assistance, noting serious limitations on assistance with the provision of bank records, with search and seizure of evidence, on restraining proceeds of crime, and on the enforcement of foreign confiscation orders.

On the terrorist financing front, the MAS has broad powers to direct financial institutions to comply with international obligations. These include UN Security Council Resolutions 1267, 1333, 1373, 1390, and other similar resolutions. In 2002, the MAS issued regulations to implement this authority. The regulations bar banks and financial institutions from providing resources and services of any kind which will benefit terrorists, and from doing "anything that . . . assists or promotes" terrorist financing. Financial institutions must notify the MAS immediately if they have in their possession, custody, or control any property belonging to terrorists or any information on transactions involving terrorists' funds. The regulations apply to all branches and offices of any financial institutions incorporated in Singapore, or incorporated outside of Singapore but which are located in Singapore. The regulations include a list of the entities and individuals on the UNSCR 1267 Sanctions Committee's consolidated list. Singapore updates the regulations periodically to include additional names as they are added by the UNSCR 1267 Sanctions Committee.

Alternative remittance systems exist, and are used mainly by the approximately 500,000 foreign workers in Singapore. All remittance agents, formal or informal, must be licensed and are subject to the same laws and regulations, including requirements for record keeping and the filing of suspicious transaction reports. In 2002, the regulations were strengthened. The firms now have to submit a financial statement every three months, and report the largest amount transmitted on a single day. Firms must also answer questions about the way they conduct business and about their overseas partners. Informal networks, such as hawala, that are not licensed are considered illegal.

Charities in Singapore are subject to extensive government regulation, including close oversight and reporting requirements, and restrictions that limit the amount of funding which can be transferred out of Singapore. A total of 1,669 charities were registered as of December 31, 2003. All charities must register with the Commissioner of Charities, and must, as part of the registration process, submit governing documents outlining the charity's objectives, and particulars on all trustees. The Commissioner of Charities has the power to investigate charities, including authority to search and seize records, and to restrict the transactions into which the charity can enter, suspend charity staff or trustees, and/or establish a scheme for the administration of the charity. Charities must keep detailed accounting records, and retain them for at least seven years.

Under the Charities (Fund-raising Appeals for Foreign Charitable Purposes) Regulations 1994, any charity or person who wishes to conduct or participate in any fund raising for any foreign charitable purpose must apply for a permit. The applicant has to show that at least 80 percent of the funds raised will be used in Singapore, although the Commissioner of Charities has discretion to allow a lower percentage to be applied within Singapore. Permit holders are subject to additional record keeping and reporting requirements, including details on every item of expenditure disbursed, amounts transmitted to persons outside Singapore, and to whom the money was transmitted.

A total of 33 permits were issued in 2003 for fund raising for foreign charitable purposes. There are not restrictions or direct reporting requirements on foreign donations to charities in Singapore.

Singapore is party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism and has signed, but has not yet ratified, the UN Convention against Transnational Organized Crime. Singapore is a member of the FATF, the Asia/Pacific Group on Money Laundering, the Egmont Group, and the Offshore Group of Banking Supervisors. Singapore will host the June 2005 Plenary meeting of the FATF, marking the first time an FATF Plenary will take place in Southeast Asia.

To bolster law enforcement cooperation and facilitate information exchange, Singapore enacted the Mutual Assistance in Criminal Matters Act (MACMA) in March 2000. The MACMA provides for international cooperation on any of the 183 predicate "serious offenses" listed under the CDSA of 1999. The provisions of the MACMA apply to countries that have concluded treaties, memoranda of understanding, or other agreements with Singapore.

In November 2000 Singapore and the United States signed the Agreement Concerning the Investigation of Drug Trafficking Offenses and Seizure and Forfeiture of Proceeds and Instrumentalities of Drug Trafficking. This was the first agreement concluded pursuant to the MACMA. This agreement, which entered into force in early 2001, facilitates the exchange of banking and corporate information on drug money laundering suspects and targets, including access to bank records. It also entails reciprocal honoring of seizure/forfeiture warrants. This agreement applies only to narcotics cases, and does not cover non-narcotics-related money laundering, terrorist financing, or financial fraud.

The Terrorism (Suppression of Financing) Act provides for mutual legal assistance in cases where there is no treaty, memorandum (MOU), or other agreement in force between Singapore and another country that is a party to the UN International Convention for the Suppression of the Financing of Terrorism. Singapore's FIU has concluded MOUs concerning cooperation in the exchange of financial intelligence with counterparts in Australia, Belgium, Japan, and the United States, and continues to actively seek MOUs with additional FIUs.

In May 2003 the Singapore Government issued a regulation pursuant to the Terrorism Act and the MACMA that enables the government to provide legal assistance to the United States and the United Kingdom in matters related to terrorism financing offenses. Singapore concluded a mutual legal assistance agreement with Hong Kong in 2003. In 2004, Singapore signed a treaty on mutual legal assistance in criminal matters with seven other members of ASEAN: Brunei, Cambodia, Indonesia, Laos, Malaysia, the Philippines and Vietnam. The treaty will come into effect after ratification by the respective governments.

The Government of Singapore should continue close monitoring of its domestic and offshore financial sectors. As a major financial center, it should also take measures to regulate and monitor large currency and bearer negotiable instrument movements into and out of the country, in line with the FATF's Ninth Special Recommendation, adopted in October 2004, that countries implement measures such as declaration systems, in order to detect cross-border currency smuggling. The conclusion of broad mutual legal assistance agreements is also important to further Singapore's ability to work internationally to counter money laundering and terrorist financing.

## **Slovak Republic**

Slovakia is not considered 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, arms, stolen vehicles, and humans. 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.

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, as well as tipping off, are criminal offenses.

As a result of amendments made to the Slovak Civil Code in 2001, new anonymous passbook savings accounts are banned. All banks in Slovakia were ordered to stop offering new anonymous accounts. All 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 accountholder for another five years. As of January 1, 2007, bearer passbook accounts will cease to exist.

In 2000 the legislature approved modifications to existing anti-money laundering regulations, with the passage of Act No. 367/2000, "On Protection against the Legalization of Proceeds from Criminal Activities." The Act came into force on January 1, 2001. One of the most significant changes that Act No. 367/2000 introduces is in relation to the types of transactions subject to the reporting requirements. The law replaces the standard of "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 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.

As recommended in 2001 by the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) 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." Act No. 367/2000 expands the list of entities subject to reporting requirements to include foreign bank subsidiaries, the Slovak Export-Import Bank, non-bank 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.

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 15,000 euros within a 12-month period is involved. (Previous law had set the reporting threshold at 2,600 euros.) Insurance sellers must identify all clients whose premium exceeds 1,000 euros in a year or whose one-time premium exceeds 2,500 euros. 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.

Originally, Slovakia's Financial Intelligence Unit (FIU), the Financial Intelligence Unit of the Bureau of Organized Crime, was established under the Ministry of the Interior and was a part of the Bureau of Financial Police (BFP). However, as of January 2004, the BFP ceased to exist and its duties were assumed by the newly created Office to Fight Organized Crime (OFOC), which 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). After the abolition of the BFP, the FIU was re-organized and moved to the OFOC.

The FIU has five primary departments: Analytical, Unusual Business Transactions, Supervision of Obligated Entities, International Cooperation, and Property Checks. The FIU increased its administrative capacity by raising its staff level from 25 to 34 personnel and its analysts participate regularly in

international and domestic fora related to combating money laundering. 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. 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. The FIU can also submit the case to the state prosecutor's office for investigation and prosecution.

In 2003, the BFP (through the FIU) registered 318 allegations of financial crime worth an estimated value of Slovak koruny (SKK) 54.8 billion (\$1.83 billion). The police formally investigated 251 of these allegations. The cases investigated had an approximate value of SKK 34.3 billion (\$1.14 billion). The police prosecuted 123 of the cases and convicted 72 entities. Also in 2003, the BFP received 489 reports alleging suspicious business operations totaling SKK 9.2 billion (\$307 million). On the basis of these 489 reports, 88 money laundering investigations were initiated by the police, resulting in the referral of 38 cases to the courts and 33 prosecutions. The BFP also conducted 23 on-site inspections of covered entities during 2003. Ten of these inspections resulted in the levying of fines totaling SKK 1,610,000 (\$54,000).

In the first eleven months of 2004, the OFOC (through the FIU) received 738 reports alleging unusual financial transactions worth a total of SKK 19.3 billion (\$643 million). It submitted 20 proposals totaling SKK 46.4 million (\$1.54 million) for criminal prosecution and 55 proposals for tax prosecution. In addition, the regional police units submitted 107 proposals for criminal prosecutions. The OFOC started 69 on-site inspections (24 are completed) of covered persons and levied penalties totaling SKK 2.41 million (\$80,300) in 23 cases.

In 2003, a law amending and supplementing the Criminal Procedure Code and Criminal Code entered into force. It provides law enforcement with the authority to conduct "sting operations" and introduces provisions regarding corporate criminal liability and "crown" witnesses. A "crown witness" (a criminal who voluntarily opts to cooperate with law enforcement bodies) could be granted immunity or receive a shortened sentence. This rule does not apply to those that organized or instigated the crime.

In late 2003, the Slovak cabinet approved a law on measures against entities that acquired property through illegal income (also known as the Law on Proving the Origin of Property). According to the draft law, an undocumented increase in property exceeding the minimum monthly wage multiplied by 200 would be scrutinized and would be considered possibly illegal. Anyone who has suspicions about possibly illegally acquired property may report it to the police, who 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. In January 2004, the Ministry of Justice withdrew the draft law from Parliament when it was evident it would not be approved.

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. All competent authorities in the Slovak Republic have full power to freeze or confiscate terrorist assets in accordance with UNSCR 1373. According to act no. 367/2000 and its later amendment, financial institutions are required to report to the regional financial police when they freeze or identify suspected terrorist-linked assets. The GOS agreed to freeze immediately all accounts owned by entities on the UNSCR 1267 Sanctions Committee's and EU's (but not the United States') consolidated lists. No terrorist finance-related accounts have been frozen or seized in Slovakia, but were a terrorism-related account to be identified, the Financial Police would 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 now a signatory to all 12 of the UN Conventions concerning the fight against terrorism. However, as reported in MONEYVAL 2004 member states' self-assessment questionnaire, Slovakia is still not fully compliant with the FATF's Special Recommendations on Terrorist Financing, having received in 2004 from MONEYVAL a rating of "partial compliance" with regard to Special Recommendation I (Implementation of UNSCR 1373) and Special Recommendation VII (enhanced scrutiny of transfers lacking originator information).

The GOS is a party to 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. However, Slovakia elected to pursue several optional terms of the convention that were fully incorporated in March 2003. The FIU has 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 2005. 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; 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. It also has signed 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 Council of Europe and participates in MONEYVAL. Slovakia sends experts to conduct mutual evaluations on fellow member countries; it also underwent mutual evaluations by this group in 1998 and 2001. Slovakia is a member of the Egmont Group.

The Government of Slovakia 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. Slovakia should also improve supervision of some non-bank sectors to ensure reporting requirements are followed. 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.

## **Slovenia**

While not a major money laundering country, Slovenia's economic stability and location on the Balkan drug route offer attractive opportunities for money laundering. Narcotics-trafficking, especially heroin via the "Balkan route" smuggled by mainly Albanian and Serbian nationals, is a growing problem and the main source of illegal proceeds. Other significant sources of illegal proceeds are fraud, trafficking in weapons and persons, and currency and securities counterfeiting, as well as extraterritorial offenses such as tax evasion, tax and VAT fraud, and corruption. Organized crime is believed to be involved in both predicate crimes and laundering operations. Money laundering often tends to be undertaken by citizens of the neighboring countries and those of the former Soviet Union, and occurs through the banking system, foreign exchange houses, real estate transactions, and cross-border currency transport.

The Penal Code criminalizes money laundering and the financing of terrorism. A change made to Slovenia's Penal Code, in 2004, increases the imprisonment penalty for money laundering from three to five years. Negligent money laundering is also criminalized.

Slovenia's Law on the Prevention of Money Laundering (LPML) was enacted in 1994 and amended in 2001 and 2002. The October 2001 amendments update the original law by, among other provisions, expanding the OMLP's sources of available financial information, and requiring mandatory client identification for transactions exceeding 3 million Slovenian tolar (approximately \$14,400). December 2001 saw the passage of a new law that increased the power of supervisory authorities to prohibit the establishment of new bearer passbook accounts and phased out already existing bearer passbook accounts. Further amendments to the law, which extend reporting obligations to lawyers, law firms, notaries, auditors and tax advisors, auctioneers, art dealers, gaming houses, and lottery concessions, were passed and entered into force in July 2002. Additional identification requirements, most notable of which is the requirement to identify beneficial owners, were also implemented. Due to the nature of their business, certain professions (lawyers, notaries, auditors, accountants, and tax advisors) are required only to file suspicious transaction reports (STRs) and are exempt from currency transaction reporting requirements. Records must be retained for a minimum of ten years. There are nine understatutory regulations in force providing detailed measures for the implementation of the LPML. Slovenian legislation is now harmonized with the provisions outlined in the Second EU Directive.



Financial supervisory bodies include the Bank of Slovenia, the Securities Market Agency, the Insurance Supervisory Agency, the Office for Gaming Supervision, the Slovene Audit Institute, and the supervisory body responsible for the oversight of tax advisory services. The Bank of Slovenia has supervisory power over bureaux de change, and in February 2003 issued a handbook for those bodies complete with reporting requirements, auditing procedures, and indicators.

Slovenia's Financial Intelligence Unit (FIU), the Office for Money Laundering Prevention (OMLP), an administrative FIU, was established in 1995 within Slovenia's Ministry of Finance. The FIU has a staff of 17. The 2002 amendments to the LPML gave OMLP more power and latitude in opening cases and sharing information. The amount of time during which transactions can be held is increased from 48 to 72 hours. The OMLP used its powers in six instances to temporarily suspend transactions with a total combined value of \$3,704,352. In its nine years of operation, OMLP has opened 764 suspicious cases and closed 655 cases. Foreign nationals were involved in more than half of these cases. In 2004, OMLP opened 112 new cases of suspected money laundering and closed 88 cases. Nine of the 88 cases were forwarded to the Police and/or Public Prosecution. In addition, 25 cases regarding suspicion of other serious criminal offenses (according to Article 22 of the LPML) were sent to the police and other competent bodies for further investigation. Two judgments have been finalized, but in both cases, due to procedural reasons, the defendants were acquitted.

Several additional cases are currently pending in the court system. The existence of a large backlog of cases in the courts continues to be a major factor impeding Slovenia's anti-money laundering regime. Law enforcement authorities, prosecutors, and judges all lack experience with regard to pursuing financial crimes, including money laundering.

The Ministry of Justice has been authorized to form a decision on whether a new law on mutual legal assistance in criminal matters will be drafted, which may include also the assets sharing provisions.

New changes and amendments (primarily focused on refining provisions regarding the financing of terrorism) are expected to be implemented after the Government of Slovenia's (GOS's) adoption of the European Union's (EU's) Third Money Laundering Directive during the second half of 2005.

The 1902 extradition treaty between the United States and the Kingdom of Serbia remains in force between the United States and Slovenia. Slovenia became a member of the EU on May 1, 2004, and is actively involved in regional efforts to combat money laundering and terrorism financing, working throughout the Balkans and Eastern Europe, especially with Serbia, Montenegro, Ukraine, Macedonia, and Russia. With regard to international cooperation, Slovenia (especially the OMLP) has a very positive reputation, having conducted a regional counternarcotics conference with Croatian counterparts, and having hosted a regional anti-money laundering conference for eight of its Balkan neighbors in October 2004.

Slovenia is a member of the Council of Europe's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), and has undergone a mutual evaluation by the Committee, as well as lending its own experts to evaluate other member countries. The OMLP is a member of the Egmont Group. Slovenia also actively participates in other multilateral programs combating money laundering and terrorism financing. Slovenia is a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime, and ratified the Civil Law Convention on Corruption in July 2003. Slovenia is also party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. In July 2003 Slovenia signed the European Convention on the Suppression of Terrorism.

The Government of Slovenia should continue to work with its law enforcement and judicial authorities to increase the levels of action and experience in pursuing financial crime. Slovenia should provide specific training to provide law enforcement, prosecutors, and judges with a better understanding of money laundering and other financial crimes so that they will be able to effectively investigate and prosecute cases of money laundering.

## **Solomon Islands**

The Solomon Islands is not a regional financial center. The Islands' banking system is small. The Parliament criminalized money laundering in 2002 with the passage of the Anti-Money Laundering Act and the Proceeds of Crime Act. The Acts provide mechanisms designed to prevent the movement of funds for terrorist purposes and to enhance the exchange of financial intelligence with other countries. Implementation of the Acts has been slow, but Parliament did act to establish a Financial Intelligence Unit (FIU) at the Central Bank in late 2004. The presence of RAMSI-affiliated Australian and New Zealand civil servants in key positions throughout the government has further aided the adoption of better banking practices.

The Solomon Islands is not a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, or the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of the Solomon Islands should become 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 should provide the recently established FIU with sufficient staff and resources to effectively carry out its mission.

## **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 and Taiwanese groups, and the Russian Mafia, have all been identified as operating in South Africa, along with native South African criminal groups. 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, 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.

The Government of South Africa (GOSA) estimates that between \$2 and \$8 billion is laundered each year through South African financial institutions. The Proceeds of Crime Act (No. 76 of 1996) criminalized 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 \$16,667,330) or imprisonment for up to 30 years. Subsequent regulations direct that the reports be sent to the Commercial Crime Unit of the South African Police Service. Both of these acts contain criminal and civil forfeiture provisions.

On November 11, 2004, the Parliament passed the Protection of Constitutional Democracy Against Terrorist and Related Activities Act (POCDATARA), which specifically criminalizes terrorist activity and terrorist financing. The Act would make it easier to identify, freeze, and seize assets related to money laundering. Significantly, the Act (which, pending Presidential signature, would take effect in early 2005) will be applicable to charitable and non-profit organizations operating in South Africa, although there is no information that these groups have been linked to terrorist financing.

In November 2001, the President signed the Financial Intelligence Centre Act (FICA) into law. Pursuant to the FICA, South Africa established both the Financial Intelligence Centre (FIC) and the Money Laundering Advisory Council to advise the Minister of Finance on policies and measures to combat money laundering. 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 began operating in February 2003. In July 2003, the FIC was admitted as a member of the Egmont Group of financial intelligence units.

The 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. Such 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, the FIC will forward 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, very few actual cases have been prosecuted to date.

From March 2003-March 2004, the FIC received 7,480 suspicious transaction reports (STRs), the vast majority from money remitters (4,079) and banks (2,732). This number was above what had been projected. Ninety percent of the STRs were sent electronically. No information is available on how many of these STRs led to criminal investigations, but the number is believed to be very low. In addition, the quality and consistency of the STRs was uneven, probably due to the fact that not all of South Africa's banks have yet implemented internal anti-money laundering training programs. Many banks believe the reporting requirements hamper their efforts to attract new customers. In particular, retroactive know your customer (KYC) requirements mean that account holders who do not present identifying documents in person risk having their accounts frozen. The National Treasury has extended the staggered timetable for fully implementing KYC (higher-risk clients first) to September 30, 2006.

The FIC made progress in 2004 in building its capabilities and in establishing its credibility with the South African law enforcement community. During its first full year of operation, it received 105 information requests from local law enforcement and 56 from international law enforcement agencies. The FIC plans to obtain further analytical training for its staff, particularly in the area of detecting terrorist financing in the absence of specific intelligence.

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. Currently, there is no legal obligation requiring alternative remittance systems to report cash transactions.

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. Those recommendations have yet to be adopted.

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. South Africa is also an active member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), having signed the memorandum of understanding in 2003.

The GOSA 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 (ratified in February 2004).

The Government of South Africa should implement the FATF recommendations to establish better control over cross-border currency movement. It should begin to regulate the country's alternative remittance systems. It should monitor and make available the number of criminal investigations resulting from STRs, and it should increase the number of actual money laundering prosecutions. It should enact and fully implement the new law against terrorist activity and terrorist financing.

## **Spain**

Money laundered in Spain is primarily from the proceeds of the Colombian cocaine trade, although money laundered through other Latin American countries also plays a role. Colombian organizations use several methods to move money from European drug sales out of Spain. Airline personnel traveling between Spain and Latin America carry out money. Colombian companies purchase goods in Asia and sell them legally at cartel-run stores in Europe. Credit card balances are paid in Spanish

banks for charges made in Latin America, or money deposited in Spanish banks is withdrawn by ATM cards in Colombia. Additionally, wire transfers continue to be a common way of getting funds out of Spain.

Drug proceeds from other regions enter Spain as well. Hashish proceeds come from Morocco and heroin money enters from Turkey. The majority of money that enters Spain to be laundered is smuggled across the border in three ways. Bulk cash is carried in travelers' luggage or hidden on their bodies when arriving at international airports; shipping containers loaded with currency enter through Spanish ports (such as Algeciras); or, money is brought in by small craft along Spain's long coastline. The informal non-bank outlets (such as "Locutorios"), which make small international transfers for the immigrant community, continue to be used to move money in and out of Spain. Regulators also suspect the presence of "hawala"-like networks in the Islamic community.

Tax evasion in internal markets and smuggling of goods along the coastline continue to be sources of illicit funds in Spain. Spanish authorities believe that tax evasion in the cell phone and property industries is the most serious problem. The smuggling of electronics and tobacco from Gibraltar remains an ongoing issue. 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.

The Government of Spain (GOS) remains committed to combating narcotics-trafficking, terrorism, and financial crimes, and continues to work hard to tighten financial controls. 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. In 1995 the law was expanded 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. To date, there have not been any cases of Spanish officials being involved in money laundering in Spain.

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.

Businesses and financial service suppliers operating in Spain or targeting Spanish markets are subject to the law, Ley de Servicios de la Sociedad de Informacion y de Comercio Electronico (LSSICE), that came into force on October 12, 2002, for Internet marketing and distribution. The new law requires businesses to register their domain names, company registry, physical address, and other company details. Financial sector businesses such as online banks must still send written contracts to new customers for signature and obtain physical proof of their identity, in order to comply with existing banking regulations.

Royal Decree 998/2003 of July 5, 2003, modified the structure of the Ministry of Interior to facilitate more active combating of drug-trafficking. This law creates an Advisory Committee on Observation that will attempt to follow the use of technologies by criminal organizations and money launderers and to take measures to ensure that Spanish law enforcement authorities are able to meet the new challenges.

Specific measures to prevent money laundering were written to regulate the legal entities in the financial sector and individuals moving large sums of cash, in December 1993 (Law No. 19/1993), as an expansion to the criminal code that previously applied only to physical persons. The regulations for enactment were established by Royal Decree 925/1995, which set the standards for regulation of the financial system. The regulations were amended in 2003 and cover money laundering linked to all serious crimes. 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.

The money laundering law applies 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 (alternative remittance systems). 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.

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. The law also requires the declaration and reporting of internal transfers of funds greater than 80,500 euros. Individuals traveling internationally are required to report the importation or exportation of currency greater than 6,000 euros. 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 Commission for the Prevention of Money Laundering and Financial Crimes (CPBC) coordinates the fight against money laundering in Spain. The Secretary of State for Economy heads the commission 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, the Federal Prosecutors (Fiscalia), Customs, the Spanish National Police, the Guardia Civil, CNMV (equivalent to the SEC), the Treasury, the Bank of Spain, and the Director General of Insurance and Pension Funds. Any member of the Commission may request an investigation, should suspicious activity be brought to his or her attention.

The CPBC 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.

The second organization is the Executive Service of the Commission for the Prevention of Money Laundering (SEPBLAC), which serves as Spain's financial intelligence unit. SEPBLAC receives and analyzes suspicious transaction reports (STRs) and currency transaction reports (CTRs). 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. Incriminating information is turned over to the federal prosecutors for prosecution. SEPBLAC received 1,351 STRs in 2002, 1,598 STRs in 2003, and 2,414 STRs in 2004. In addition, SEPBLAC received 205,252 CTRs in 2002, 294,508 CTRs in 2003, and 331,856 CTRs in 2004.

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 half going to drug treatment programs and half to a foundation that supports the officers fighting narcotics-trafficking. Seizures of assets involving more than one country, and the division of the assets, depend on the relationship with the country in question. EU working groups will 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.

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. The commission is headed by the Ministry of Interior, and includes representatives from the Fiscalia and Ministries of Justice and Economy. SEPBLAC will serve as the Executive Service and as the Secretariat for this Commission. Currently, only the head of CVAFT can request information in terrorist financing cases, so other members must rely on the commission head to begin an investigation.

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. The 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 goes beyond EU requirements. However, the implementing regulations for this law have not been written, and it has not been used. Once in full effect, this law will allow administrative freezing of suspect assets without a judge's order.

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.

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. The GOS is a party to the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of the Financing of Terrorism. Spain is also a party to the 1988 UN Drug Convention. SEPBLAC is a member of the Egmont Group and is currently chairing one of the Egmont Committee working groups.

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 also has entered into bilateral agreements for cooperation and information exchange on money laundering issues with Bolivia, Chile, El Salvador, France, Israel, Italy, Malta, Mexico, Panama, Portugal, Russia, Turkey, Venezuela, Uruguay and the United States. SEPBLAC has also entered into bilateral agreements for cooperation and information exchange on money laundering issues with Andorra, Argentina, Australia, Belgium, Brazil, Bulgaria, Colombia, Finland, France, Guatemala, Italy, Korea, Mexico, Monaco, Panama, Peru, Poland, Portugal, Romania, Ukraine, Venezuela and the United States. Spain actively collaborates with Europol, supplying and exchanging information on terrorist groups. U.S. law enforcement agencies reported excellent cooperation with their Spanish counterparts in 2004. U.S. customs works closely with Spanish customs, Spanish prosecutors, the national police corps and the Civil Guard. The Drug Enforcement Administration works closely with SEPBLAC, the national police and the Civil Guard. These organizations regularly share information. Official documents however, will only be transferred if requested by a court.

The scale of the money laundering industry and the sophisticated methods used by criminals create a very large law enforcement problem in Spain. The Government of Spain makes every effort to eliminate financial crime in the country. Spain should continue the strong enforcement of its anti-money laundering program and its leadership in the international arena. It should consider whether additional measures are required to address possible money laundering in the stock market to ensure that the sector is not used for financial crimes and should fully implement Law 12/2003 to allow administrative freezing of suspect assets.

## **Sri Lanka**

Sri Lanka is neither an important regional financial center nor a preferred center for money laundering. Money laundering currently is not a criminal offense. There are strict bank secrecy laws, under which the Government of Sri Lanka is required to obtain a court order to obtain banking information on bank customers. The Central Bank introduced regulations on customer due diligence in a December 2001 bid to tackle money laundering and terrorist financing in the absence of a specific legal framework. These regulations apply to commercial banks and licensed specialized banks coming under the Central Bank. The Government is in the process of finalizing draft legislation to deal with money laundering and terrorist financing. There are three draft laws under discussion: a law to prohibit money laundering and to provide for measures to combat money laundering; a law to give effect to the UN International Convention for the Suppression of the Financing of Terrorism; and a financial transaction reporting law modeled on those in the Commonwealth which will provide, among other things, for the establishment of a financial intelligence unit. There has been a delay in finalizing the legislation as the

GSL debates what sort of presumptions to establish with respect to innocence or guilt. Currently, financial transactions relating to terrorism and narcotics are illegal under Central Bank regulations and banking laws.

The definition of money laundering, under the proposed anti-money laundering law covers (as predicate offenses) the offenses under existing and proposed laws on narcotics, terrorism prevention, bribery, firearms, exchange control, transnational organized crime, cyber crimes, child protection and trafficking of persons and any other offense punishable by death or imprisonment of seven years or more. The offense of money laundering involves receiving, possessing, concealing, investing, disposing of, importing, exporting, or dealing in any property or proceeds derived or realized from any unlawful activity covered by the law. Under the sentencing provisions of the proposed anti-money laundering law, persons convicted will be liable for a fine and imprisonment for a period of 5-20 years. Under the sentencing provisions of the proposed counterterrorist financing law, persons convicted will be liable for a fine and imprisonment for a period of 15-20 years. Under the proposed laws, both money laundering and terrorist financing would be extraditable offenses.

Many areas of concern exist with respect to Sri Lanka's current anti-money laundering efforts. The Central Bank continues to allow the operation of bearer certificates of deposits. In July 2003, in order to limit money laundering through bearer certificates, the Central Bank required banks to maintain a record of purchasers of these certificates. Another area of concern relates to a 2003 tax amnesty, under which Sri Lankan individuals and companies could declare previously undisclosed wealth accrued from any source and receive immunity from a range of taxes. The amnesty was revised recently, so that immunity is now only available with respect to the payment of income tax on relevant funds. Casinos, jewelry shops and dealers in gems are also areas of concern, as there is no law to regulate their operations. Sri Lanka has also become a transit point for illegal migration of Sri Lankans and other Asian nationals to Europe, North America and the Gulf.

Sri Lanka has an indigenous alternative remittance system in the form of informal money transfer operations. Many Sri Lankan migrant workers, mainly in the Middle East, use a hawala-like system to remit their earnings. Various payments out of Sri Lanka are also made using this system. Sri Lankan commercial banks are increasing their presence and services in the Middle East in order to cater to this clientele. Trafficking of drugs generates significant amounts of criminal proceeds, and those proceeds are also readily transported using this system. Drug proceeds are laundered through various methods, including investment in real estate.

Sri Lanka is not considered an offshore financial center. Offshore banking units are allowed to operate as a part of a commercial bank operating in an overseas country in order to facilitate trade finance. They are subject to Central Bank supervision. Bearer shares are not permitted for offshore banks and foreign-owned companies. Sri Lanka has 10 free trade zones, also called export-processing zones, administered by the state-owned Board of Investment (BOI). The free trade zones house export-manufacturing operations. Only companies approved by the BOI are allowed to operate inside the zones. There are no indications that these free trade zones are being used in trade-based money laundering schemes or terrorist financing.

Sri Lanka is a party to the UN International Convention for the Suppression of the Financing of Terrorism and to the 1988 UN Drug Convention. Sri Lanka has signed but not ratified the UN Convention against Transnational Organized Crime. Sri Lanka is a member of the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC) working group on Counter-Terrorism and Transnational Crime formed in July 2004. The working group had its first meeting in December 2004 and aims to serve as a platform for regional cooperation to prevent and suppress terrorism and transnational crime.

The Mutual Assistance in Criminal Matters Act of 2002 provides for cooperation in criminal matters with Commonwealth countries. According to the law, additional bilateral agreements on mutual assistance in criminal matters are required for extending provisions of the act to non-Commonwealth countries. Under the proposed law to give effect to the UN International Convention for the Suppression of the Financing of Terrorism, the government is required to co-operate and provide assistance to states party to the Convention with regard to investigations and prosecutions under the law. The Central Bank of Sri Lanka has circulated the list of individuals and entities that have been

included on the UNSCR 1267 Sanctions Committee's consolidated list with instructions to identify, freeze and seize terrorist assets. To date, no such assets have been identified.

Terrorist financing is an offense punishable by imprisonment for a period of five to ten year. Regulations under the United Nations Act No. 45 of 1968 provide for the freezing and forfeiture of assets of financiers of terrorism. There is no specific provision in law for the freezing and forfeiture of narcotics-related assets. The trafficking, possessing, importing or exporting of narcotics is punishable by death or life imprisonment under the Poisons, Opium and Dangerous Drugs Ordinance (OPDDO). Draft amendments to OPDDO, and new money laundering and terrorist financing legislation include asset forfeiture and seizure provisions for narcotics related crimes, money laundering and terrorist financing.

The Government of Sri Lanka should act on the three draft laws referred to above and initiate a comprehensive anti-money laundering program that has as its foundation anti-money laundering and counterterrorist financing laws. The property and proceeds arising out of all serious crime should be included as predicate offenses for money laundering. The practice of permitting bearer certificates of deposit should be terminated. There should be a formalized system of reporting suspicious transactions from financial institutions to a Financial Intelligence Unit (FIU). Casinos should also be made subject to financial intelligence reporting to the FIU. Sri Lanka should devote adequate resources to train police and customs officials to recognize and investigate different forms of money laundering, including alternative remittance systems. Sri Lanka should ratify the UN Convention against Transnational Organized Crime.

### **St. Kitts and Nevis**

The Government of St. Kitts and Nevis (GOSKN) is a federation composed of two islands in the Eastern Caribbean, but each island has the authority to organize its own financial structure. The federation is at major risk for corruption and money laundering, due to the high volume of narcotics-trafficking activity through and around the islands and the presence of known traffickers on the islands. An inadequately regulated economic citizenship program adds to the problem.

Most of the offshore financial activity in the federation is concentrated in Nevis, in which there is one offshore bank (a wholly owned subsidiary of a domestic bank), approximately 15,000 international business companies (IBCs), and 950 trusts. The Nevis domestic structure consists of five domestic banks, four domestic insurance companies (all of which are subsidiaries of St. Kitts companies), and two money remitters. There are also 50 trust and company service providers. In 2003 St. Kitts had four domestic banks, 120 credit unions, four domestic insurance companies, two money remitters, and 15 company service providers. There are also four trusts, one casino, and 450 exempt companies. Applicants may apply as an IBC for an Internet gaming license; however, none were issued in 2003. The GOSKN did not release statistics for 2004. St. Kitts claims to have no Internet gaming operations.

The Proceeds of Crime Act No. 16 of 2000 criminalizes money laundering for serious offenses (defined to include more than drug offenses) and imposes penalties ranging from imprisonment to monetary fines. The Act 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 measures designed to remedy shortcomings in St. Kitts and Nevis' anti-money laundering regime include the Financial Services Commission Act No. 17 of 2000, the Nevis Offshore Banking (Amendment) Ordinance No. 3 of 2000, the Anti-Money Laundering Regulations No. 15 of 2001, the Companies (Amendment) Act No. 14 of 2001, the Anti-Money Laundering (Amendment) Regulations No. 36 of 2001, the Nevis Business Corporation (Amendment) Ordinance No. 3 of 2001, and the Nevis Offshore Banking (Amendment) Ordinance No. 4 of 2001.

A regional stock exchange, common to the members of the Organization of Eastern Caribbean States and supervised by a regional regulator, is located in St. Kitts. The Eastern Caribbean Central Bank has direct responsibility for regulating and supervising the offshore bank in Nevis, as it does for the entire domestic sector of St. Kitts and Nevis (SKN), and for making recommendations regarding approval of offshore bank licenses. The St. Kitts and Nevis Financial Services Commission, with regulators on both islands, regulates non-bank financial institutions for anti-money laundering compliance.



The GOSKN also issued regulations requiring financial institutions to identify their customers, to maintain a record of transactions, to report suspicious transactions, and to 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's Regulator is authorized to carry out anti-money laundering examinations. The GOSKN has separated the offshore marketing and regulatory functions. In particular, an offshore Marketing and Development Department, separate from the Financial Services Commission, was established in April 2001. Legislation requires certain identifying information to be maintained about bearer certificates, including the name and address of the bearer of the certificate, as well as its beneficial owner. In addition to these measures, Nevis issued regulations aimed at facilitating the identification of beneficial owners of corporations and corporate shareholders.

The Financial Intelligence Unit Act No. 15 of 2000 authorizes the creation of the Financial Intelligence Unit (FIU). The FIU began operations in 2001 and has a new director, deputy director, and four police officers. The FIU receives, collects, and investigates suspicious activity reports (SARs). The FIU is also charged with liaising with foreign jurisdictions. By November 2003, the FIU had received 77 SARs. No figures were released for 2004. During its first two years of operation the FIU received over 100 SARs and froze over \$1.6 million.

Financial Services (Exchange of Information) Regulations were promulgated in 2002. These regulations define the parameters for the exchange of information between domestic regulatory agencies and foreign regulatory agencies. Financial services officials in SKN have been seeking to educate relevant stakeholders as to their responsibilities related to anti-money laundering, using radio, television, newspapers, and seminars. The GOSKN encouraged the founding of an association of compliance officers within relevant financial institutions, and provided training in anti-money laundering to government financial services personnel. In 2003, the Nevis island administration announced plans to strengthen regulatory oversight of service providers.

St. Kitts and Nevis enacted the Anti-Terrorism Act No. 21, effective November 27, 2002. Sections 12 and 15 of the Act criminalize terrorist financing. The Act implements various UN Conventions against terrorism. The GOSKN has some existing controls that apply to alternative remittance systems, but has undertaken no initiatives that apply directly to the potential terrorist misuse of charitable and nonprofit entities. St. Kitts and Nevis circulates lists of terrorists and terrorist entities to all financial institutions. To date, no accounts associated with terrorists or terrorist entities have been found in SKN.

A mutual legal assistance treaty between SVN and the United States entered into force in early 2000. 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 Experts Group to Control Money Laundering (OAS/CICAD). St. Kitts and Nevis is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism, and on May 21, 2004, ratified the UN Convention against Transnational Organized Crime.

The Government of St. Kitts and Nevis continues to be vulnerable to money laundering and other financial crimes. St. Kitts and Nevis should continue to devote sufficient resources to effectively implement its anti-money laundering regime. Specifically, St. Kitts and Nevis should determine the number of Internet gaming sites present on the islands. Oversight of these entities is crucial, as they are vulnerable to abuse by criminal and terrorist groups. Additionally, St. Kitts and Nevis should curtail its economic citizenship program.

## **St. Lucia**

St. Lucia has developed an offshore financial service center that could potentially make the island more vulnerable to money laundering and other financial crimes.

Currently, St. Lucia has five offshore banks, 1,438 international business companies, 33 international trusts, 17 international insurance companies, two money remitters, three mutual fund administrators, 9 registered agents and 3 registered trustees (service providers) and six domestic banks. St. Lucia has

a free trade zone. The Government of St. Lucia (GOSL) also is considering the establishment of gaming enterprises.

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. 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 (ML Prevention Act), which criminalizes the laundering of proceeds with respect to 15 prescribed offenses, including narcotics-trafficking, corruption, fraud, terrorism, gambling and robbery. The ML Prevention Act mandates suspicious transaction reporting requirements and imposes record keeping requirements. In addition, the ML Prevention Act 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."

Pursuant to the ML Prevention Act, the Money Laundering (Prevention) Authority (the Authority) was established in early 2000. The Authority consists of five persons "who have sound knowledge of the law, banking or finance." The Authority's functions include receipt of suspicious transaction reports, subsequent investigation of the transactions, dissemination of information within (e.g., to the Director of Public Prosecutions) or outside of St. Lucia, and monitoring of compliance with the law. The ML Prevention Act imposes a duty on the Authority to cooperate with competent foreign authorities. Assistance includes the provision of documents, testimony, conduct of examinations, execution of search and seizure orders, and the provision of information and evidentiary items. The Authority has a number of regulatory powers, including the right to enter the premises of a financial institution during normal working hours to inspect transaction records or copy relevant documentation, to issue guidelines to financial institutions, and to instruct a financial institution to facilitate an investigation by the Authority.

In 1999, the GOSL also 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 funds business may not be registered without the approval of the Minister responsible for international financial services. An IBC may be struck off the register on the grounds of carrying on business against the public interest.

The Financial Intelligence Authority Act No. 17 of 2002 authorizes the establishment of a Financial Intelligence Unit (FIU) for St. Lucia, which became operational in October 2003. Some functions of the Authority have been transferred to the new FIU. The FIU is able to compel the production of information necessary to investigate possible offenses under the 1993 Proceeds of Crime Act and the ML Prevention Act. 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 Caribbean Anti-Money Laundering Program (CALP) has trained St. Lucia's FIU personnel. In September 2003, legislation was adopted merging the Authority with the FIU. In December 2004, the FIU received 25 suspicious transaction reports. There have been

no money laundering convictions to date in St. Lucia. However, there is a money laundering case pending.

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. The Eastern Caribbean Central Bank regulates St. Lucia's domestic banking sector.

Counterterrorism and counterterrorist financing legislation is pending before the St. Lucia Parliament. In 2002, St. Lucia signed the Inter-American Convention Against Terrorism, which includes counterterrorist financing provisions. St. Lucia circulates lists of terrorists and terrorist entities to all financial institutions. 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.

As a member of the Caribbean Financial Action Task Force (CFATF), St. Lucia underwent a First Round Mutual Evaluation immediately prior to the establishment of its offshore sector. St. Lucia underwent its Second Round evaluation in September 2003. St. Lucia is a member of the OAS Inter-American Drug Abuse Control Commission (OAS/CICAD) Experts Group to Control Money Laundering. 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. The GOSL has been cooperative with the USG in financial crime investigations. St. Lucia is a party to the 1988 UN Drug Convention and, on September 26, 2001, signed, but has not yet ratified, the UN Convention against Transnational Organized Crime. The GOSL has not signed the UN International Convention for the Suppression of the Financing of Terrorism.

The Government of St. Lucia should become a party to the UN International Convention for the Suppression of the Financing of Terrorism and adopt counterterrorism financing legislation. St. Lucia should continue to enhance and implement its money laundering legislation and programs.

### **St. Vincent and the Grenadines**

St. Vincent and the Grenadines remains vulnerable to money laundering, other financial crimes, and the facilitation of terrorist financing, as a result of the rapid expansion and inadequate regulation of its offshore sector. The offshore sector includes 11 offshore banks, 6,276 international business corporations, 11 offshore insurance companies and 153 international trusts. The domestic sector comprises two commercial banks, a development bank, two savings and loan banks, a building society, 13 insurance companies, 10 credit unions, and two money remitters. There are no free trade zones in St. Vincent and the Grenadines (SVG) nor have any Internet gaming licenses been issued. The Eastern Caribbean Central Bank (ECCB) supervises SVG's four domestic banks. Beginning in October 2001 with an administrative agreement, and finalized in the International Banks (Amendment) Act No. 30 of 2002, the Government of St. Vincent and the Grenadines (GOSVG) gave the ECCB increasing authority to review and make recommendations regarding approval of offshore bank license applications, and to directly supervise the offshore banks in cooperation with the GOSVG's Offshore Finance Authority (OFA). The agreement includes provisions for joint on-site inspections to evaluate the financial soundness and anti-money laundering programs of offshore banks. The OFA alone continues to supervise and regulate the other offshore sector entities; however, its staff exercises only rudimentary controls over these institutions. The GOSVG has strengthened the structure and staffing of the OFA by appointing five new members to the OFA board. This brings the total to 12 staffers to regulate offshore insurance and mutual funds.

In June 2003, the Financial Action Task Force (FATF) recognized that the GOSVG, through enactment and implementation of appropriate legal reforms, had sufficiently addressed deficiencies identified by the FATF in 2000, and removed it from the list of Non-Cooperative Countries or

Territories (NCCT). With SVG's removal from the NCCT list, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) lifted its advisory, which had instructed all U.S. financial institutions to "give enhanced scrutiny" to all transactions involving St. Vincent and the Grenadines. The FATF encouraged the GOSVG to consider tightening provisions relating to the granting of exemptions from customer identification requirements.

Since July 2000, the GOSVG has passed substantial legislation, primarily the International Banks (Amendment) Act No. 7 of 2000 that deals with the authorization and regulation requirements for offshore banks as well as with the rules regarding the transfer of shares and beneficial interest. The GOSVG also enacted the International Banks (Amendment) Act of October 2000, which enables the Offshore Finance Inspector to have 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. The GOSVG prepared a further amendment to the International Banks Act with a view to improving licensing procedures and better regulating the offshore banking sector.

The GOSVG enacted the Proceeds of Crime and Money Laundering (Prevention) Act in December 2001 and the Proceeds of Crime (Money Laundering) Regulations in January 2002. Subsequent amendments further strengthen provisions of the Act and the Regulations. Among other measures, the Act criminalizes money laundering and imposes on financial institutions and regulated businesses a requirement to report suspicious transactions likely to be related to money laundering or the proceeds of crime. The related regulations establish mandatory record keeping rules and limited customer identification/verification requirements.

The GOSVG enacted the International Business Companies Amendment Act No. 26 of 2002, which became effective on May 27, 2002, to immobilize and register bearer shares. The GOSVG also revoked the Confidentiality Act and passed the Exchange of Information Act No. 29 of 2002 to authorize and facilitate the exchange of information, particularly among regulatory bodies. In April 2001, the GOSVG revoked its economic citizenship program, which provided the legal basis to sell citizenship and passports, although there were no reports of passports having been issued under the program.

The Financial Intelligence Unit Act No. 38 of 2001 (FIU Act) establishes the Financial Intelligence Unit (FIU) that began operation in May 2002. The FIU Act allows for the exchange of information with foreign FIUs. An amendment to the FIU Act permits the sharing of information even at the investigative or intelligence stage. The FIU has a staff of 14 and became a member of the Egmont Group in June 2003. As of October 2004, the FIU had received 88 suspicious activity reports for the year and almost 400 since its inception. In November 2004, the FIU began an anti-money laundering /counterterrorist finance training initiative at the financial institutions.

There have been no money laundering convictions, but the GOSVG has frozen approximately \$1.5 million and confiscated approximately \$40,000. Officials also cooperated with a U.S. investigation of a major suspected money launderer in 2002. In 2003, the GOSVG reintroduced a customs declaration form to be completed by incoming travelers. Incoming travelers are required to declare currency over approximately \$3,800.

The GOSVG enacted the United Nations Terrorism Measures Act No. 34, effective August 2, 2002. Sections 3 and 4 of the Act criminalize terrorist financing. The GOSVG has not undertaken any specific initiatives focused on the misuse of charitable and nonprofit entities. 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 is a member of the Caribbean Financial Action Task Force, and underwent its Second Round mutual evaluation in November 2002. In addition, the GOSVG is a member of the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD). The GOSVG is a party to the 1988 UN Drug Convention and acceded to the Inter-American Convention against Corruption in 2001. The GOSVG signed, but has not yet ratified, the UN Convention against Transnational Organized Crime. The GOSVG is a party to the UN International Convention for the Suppression of the Financing of Terrorism and is deemed to be partially compliant with its requirements. An updated extradition treaty and a Mutual Legal Assistance

Treaty between the United States and the GOSVG entered into force in September 1999. The FIU executes the Mutual Legal Assistance Treaty requests.

The Government of St. Vincent and the Grenadines should address all remaining concerns raised by the international community in regard to its anti-money laundering regime. These include the areas of customer identification, money remitters, outstanding bearer shares, and money laundering prosecutions. St. Vincent and the Grenadines should continue to provide training to its regulatory, law enforcement, and Financial Intelligence Unit personnel in money laundering operations and investigations. St. Vincent and the Grenadines also should ensure that it properly supervises the offshore sector. St. Vincent and the Grenadines should pass counterterrorist financing legislation that will provide the authority to identify, freeze and seize terrorist assets.

## **Suriname**

Suriname is not a regional financial center. Narcotics-related money laundering occurs primarily through unregulated private sector activities, specifically casinos, gold mining and car dealerships. Narcotics-related money laundering is closely linked to transnational criminal activity related to the transshipment of Colombian cocaine and is believed to occur through both the non-banking financial system (i.e., money exchange businesses or cambios) and through a variety of other means including, but not limited to, the sale of gold purchased with illicit money and the manipulation of commercial and state-controlled bank accounts. Both local drug-trafficking organizations and organized crime are believed to control the money laundering proceeds. Suriname does not have an offshore sector nor free trade zones.

Although Suriname's overall anti-money laundering regime still remains weak, it made significant progress in 2004. A package of anti-money laundering legislation passed in 2002 by the Government of Suriname (GOS) is based on recommendations made by the Caribbean Financial Action Task Force (CFATF). This legislation addresses multiple issues including (a) criminalizing money laundering, (b) establishing a Financial Intelligence Unit (FIU) to track and report on unusual and suspicious financial transactions, and (c) requiring financial service providers to store information on clients for seven years and to confirm the identities of clients, individual or corporate, before completing requested financial services. The legislation includes a due diligence section making individual bankers responsible if their institution is laundering money, and ensures the protection of bankers and others with respect to their cooperation with law enforcement officials. The law, "Reporting of Unusual Transactions," enacted in September 2002, entered into force in March 2003. This law requires financial institutions, other intermediaries and natural legal persons who conduct financial services to report suspicious financial transactions to the FIU.

In addition, there is an amendment to the criminal code allowing authorities to confiscate illegally obtained proceeds and assets obtained partly or completely through criminal offenses. There are no provisions for civil forfeiture, and there is no legal mechanism that designates the proceeds gained by the sale of forfeited goods to be used directly for law enforcement efforts.

The Central Bank issued guidelines for the prevention of money laundering in 1996 that contain a definition of a suspicious transaction as any transaction that deviates from the usual account and customer activities and that are not "normal" daily banking business. These guidelines are not mandatory.

The FIU opened an office in early 2003, and personnel received extensive training in 2004. The FIU, which falls under the auspices of the Attorney General's office, is tasked with identifying, recording and reporting the identity of customers engaging in suspicious financial transactions. After an initial rough start, when the head of the FIU resigned effective January 2004 after less than six months in office, the FIU is making progress under a new director.

Suriname's financial regime was challenged in early 2004 by a currency change which dropped three zeros from the currency and changed the name from the Surinamese Guilder to the Surinamese Dollar. Anticipating problems, the Central Bank required that suspicious transactions be reported/investigated. The FIU, however, did not detect any suspicious transactions from commercial

banks related to the exploitation of the change in currency. The FIU, however, did not receive information from currency exchange cambios.

Suriname's money laundering regime was further enhanced in 2004 with the establishment of a Financial Investigation Team (FOT) within the Attorney General's office. The FOT is responsible for investigating suspicious transactions discovered by the FIU. The results of the investigation are then sent to the police and prosecutor's office to be used as prosecutorial evidence. In November a Surinamese judge convicted a money laundering suspect for the first time in a landmark court case, marking the first successful implementation of Suriname's 2002 anti-money laundering law. Both the FIU and FOT were instrumental in providing sufficient evidence to ensure a conviction. The suspect, whose country of origin is unknown, received a seven-year prison sentence for intentional money laundering and attempting to export a small amount of cocaine.

Resource constraints and in particular a severe shortage of judges will be a limiting factor in expanding this judicial success. A new class of nine judges, in training, will partially redress the problem, but they will not complete training for another four to five years.

The GOS has not criminalized terrorist financing. However, GOS officials are working with the Caribbean Anti-Money Laundering Program to draft legislation requiring transparency in the financial sector that would contain specific provisions for terrorist financing.

The GOS has an agreement with the Netherlands on extradition and legal assistance with regard to criminal matters, but extradition of Surinamese nationals is prohibited. Suriname also has bilateral treaties and cooperation agreements with the United States, on narcotics-trafficking, and with Colombia, France and Netherlands Antilles on transnational organized crime. Suriname is a member of the CFATF and the Organization of American States Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD). Suriname is party to the 1988 UN Drug Convention and signed the Inter American Convention against Terrorism in June 2002, but has not yet ratified it.

The Government of Suriname should continue its efforts to fully implement its anti-money laundering legislation, particularly through expansion of the Financial Intelligence Unit (FIU) and Financial Investigation Team (FOT) and further training of personnel. Suriname should criminalize terrorist financing and become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

## **Swaziland**

Swaziland is a growing regional financial center. International narcotics-trafficking, primarily in marijuana, continues to grow in Swaziland. The country's proximity to South Africa, lack of effective counternarcotics legislation, limited enforcement resources, relatively open society and developed economic infrastructure make it attractive for trafficking organizations and increase the risk for money laundering.

The Central Bank of Swaziland and the Ministry of Finance are currently drafting an amendment to the Money laundering Act of 2001 (the Act). Although the Act criminalizes money laundering for specified predicate offenses, including narcotics-trafficking, kidnapping, counterfeiting, extortion, fraud, and arms trafficking, it does not adequately address processes and procedures for the police to follow when money laundering is suspected. The penalty for money laundering is six years imprisonment, a fine amounting to roughly \$3,500, or both. The Act establishes a currency reporting requirement, requires banks to report suspicious transactions to the Central Bank, and provides conditions when assets may be frozen and forfeited. The Act also requires banks to retain records for five years, to improve the ability to trace suspicious transactions and patterns.

On November 16, 2004, the Central Bank of Swaziland and the Bankers Association of Swaziland issued a general statement on anti-money laundering regarding the importance of positive identification in banking. The statement says that Swaziland's financial institutions will not conduct transactions with any customers failing to furnish proof of their identity and that service shall not be

provided when there is any reason to suspect that money laundering may be involved. By June 30, 2005, all existing customers of Swaziland's financial institutions will need to present current information to establish their actual identity.

To assist the banking community with tracking suspicious transactions, the Central Bank distributed anti-money laundering guidelines to all banks in late 2002. As of December 2004, the Central Bank received fewer than 10 reports of suspicious transactions. The police bear responsibility for investigating such cases, but no investigations have taken place—one reason the Central Bank and the Ministry of Finance are amending the 2001 Act. The police also would be responsible for seizing any assets related to money laundering, but no seizures have taken place under the Act.

Members of the Royal Swaziland Police Service (RSPS) have noted that they lack the ability to understand and monitor small businesses. The RSPS has little liaison or cooperation with those ministries of the Government of the Kingdom of Swaziland (GKOS) involved with regulating businesses and business owners. Their expressed concerns in this arena include a perceived escalation in the number of foreign business owners throughout Swaziland. While the RSPS is becoming aware that businesses, such as used car lots, cellular and electronic shops, and sundries stores, are commonly used throughout the world as fronts and/or laundering mechanisms, the RSPS lacks the inter-departmental infrastructure and agreements to address this growing concern. Simply stated, the small business sector in Swaziland has been traditionally overlooked as a very real potential money laundering and support element for drug traffickers and terrorist groups. More inter-departmental and inter-ministerial cooperation is needed in order to properly assess and address this vulnerability.

The Act allows for providing assistance to foreign countries that have entered into mutual assistance treaties with the GKOS. An amendment to the Act will allow for Swaziland to comply with regional agreements and international conventions.

Swaziland is party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. The GKOS has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. Swaziland is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), a FATF-style regional body. Swaziland served as President of ESAAMLG from August 2002 to August 2003.

The Government of the Kingdom of the Swaziland (GKOS) should criminalize terrorist financing. Swaziland should also establish an anti-money laundering regime consistent with international standards, including a financial intelligence unit capable of sharing information with foreign law enforcement and regulatory officials. The Kingdom of the Swaziland should provide the appropriate resources and training to its law enforcement personnel to allow them to adequately perform their duties.

## **Sweden**

Sweden does not appear to have a significant money laundering problem. Swedish anti-money laundering legislation includes all serious crimes, and the money laundering controls allow Sweden to fulfill the recommendations of the Hague Forfeiture Convention. The 2004 Transparency International Corruption Perception Index lists Sweden as the sixth (perceived) least corrupt country. Sweden relies on transparency of institutions to keep corruption at bay; however the focus on corruption has been increasing over the past few years. In January of 2004, two Swedish consultants were convicted of bribing foreign public officials at the World Bank. The court's decision has been appealed, but this decision marks the first bribery case of a foreign public official ruled on in a Swedish court.

Among the Nordic countries, Sweden has the highest number of money laundering reports. One reason is that Sweden, in comparison with other Nordic countries, has more currency exchange offices, which appear to be the preferred mechanism for money laundering. Other financial institutions, such as postal giro companies, are also used to launder money. A new trend identified by the Financial Police concerns large cash withdrawals by entrepreneurs on the illegal labor market, especially in the construction and cleaning business sectors. The money primarily emanates from narcotics, tax fraud, economic crimes and robbery.

Swedish law requires banks, credit market companies, securities businesses, exchange offices, remittance dealers, insurance brokers, life insurance companies, and casinos to report suspicious activity to the police Financial Intelligence Unit (FIU). The law also requires financial institutions, insurance companies, securities firms, currency exchange houses, providers of electronic money, and money transfer companies to verify customer identification, inquire into a transaction's background, and verify identities for each transaction, particularly in the case of new customers and involving amounts above SEK 110,000 (approximately \$16,300). Banks and financial institutions are obliged to observe and report to the police transactions that are suspected to include funds that will be used to finance serious crimes. Swedish law does not allow individual officers of covered institutions to be penalized for noncompliance; however, the Swedish Supervisory Authority has the ability to sanction noncompliant institutions.

Sweden implemented new regulations to further comply with the 1991 European Union (EU) Directive on Money Laundering approved in 2001. According to the new regulations the FIU is entitled to demand customer information from accounting firms; law firms; tax counselors; casinos; real estate brokers; dealers in antiques, jewelry, and art; companies buying and selling new and used vehicles; and firms dealing with gambling and the sale of lottery tickets. The new regulation came into effect on January 1, 2005. Sweden's FIU received 4,155 suspicious transaction reports in 2001, a 60 percent increase from 2000 due to the implementation of the EU's Anti-Money Laundering Directive through Swedish law, which requires bureaux de change to report suspicious activity. The FIU received 8,008 suspicious transaction reports in 2002, 10,000 reports in 2003, and 9,929 reports in 2004. The Financial Police believe that increase in suspicious activity is attributed to Baltic countries' entrance into the EU.

The number of prosecutions in Sweden has been relatively low. In 2003, only four cases were brought to trial and resulted in conviction. During 2004, the number was similar. Suspected money laundering in Sweden requires a full investigation of the initial crimes to fully establish the origin of the money. This has proven to be a difficult and resource-consuming effort, which results in fewer prosecutions. The law on money laundering stipulates six months to two years in prison. The average time in prison for perpetrators convicted of money laundering is around one year.

Sweden ratified the International Convention for the Suppression of the Financing of Terrorism on June 6, 2002, and on July 1, 2002, a new act on penalties for financing serious crimes entered into force. According to the act, it is a punishable crime to collect, provide, or receive money or other funds with the intention that they be used, or with the knowledge that they are to be used, to commit actions that constitute offenses under the international counterterrorism conventions. Attempts to commit such crimes are also punishable. Sweden has had two cases under this law but neither went to trial. One reason was that the actual amount involved was too low to prosecute. Another reason related to difficulties in prosecuting under the law. The prosecutor has to be able to prove intent to fund not only a particular organization, but also the intent to fund a terrorist activity. Three Swedish citizens were put on the terrorist list by the U.S., and then approved by the UN and later also by the EU, since they had connections to the bank al-Barakhaat. Two have been taken off the list but the third, Ahmed Yusuf, is still on the list.

Swedish law also provides for the seizure of assets derived from drug-related activity, however, it is not possible to stop a transaction based solely on suspicions of unlawful activity. Law enforcement officials may only seize the assets of an organization or individual that is the subject of an ongoing criminal investigation. Freezing of assets based on UN Security Council Resolutions is carried out by implementation of EC law. UN and international sanctions can be imposed through the 1995 Sanctions Act, however, the Swedish government does not have the authority to identify potential sources of terrorist financing and to disrupt them on its own without a decision by the EU or UN.

Sweden has endorsed the Basel Committee's "Core Principles for Effective Banking Supervision." Sweden is a member of the Financial Action Task Force (FATF), serving as the Chair for 2004, and the Council of Europe. Its FIU is a member of the Egmont Group. Sweden is a party to the 1988 UN Drug Convention and on April 30, 2004, ratified the UN Convention against Transnational Organized Crime. It is also a party to the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. Sweden has signed, but not yet ratified, the UN Convention against Corruption.



The Government of Sweden should continue to expand its anti-money laundering/counterterrorist financing regime. Sweden should adopt reporting requirements for the cross-border transportation of currency or monetary instruments. Sweden should ensure that legislation is enacted to extend suspicious transaction reporting requirements to intermediaries, such as attorneys, accountants, and financial advisors and to ease the difficulties proving and prosecuting the crime of money laundering.

## **Switzerland**

Switzerland is a major international financial center, with some 370 banks maintaining headquarters there. In addition, approximately 12,000 to 15,000 fiduciaries function as non-bank financial institutions. Narcotics-related money laundering proceeds are largely controlled by foreign drug-trafficking organizations. Authorities suspect that Switzerland is vulnerable at the layering and integration stages. 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 are all factors that make Switzerland a major international financial center. These same factors make Switzerland attractive to potential money launderers. However, Swiss authorities are aware of this and are sensitive to the size of the Swiss private banking industry relative to the size of the economy, and waive bank secrecy rules in the prosecution of money laundering and other criminal cases. Deposits in Swiss institutions represent an estimated \$2.9 trillion, with foreigners accounting for over half of the input into the financial system; this amount is 12 times the GDP of the country.

Reporting indicates that criminals attempt to launder proceeds in Switzerland from a wide range of illegal activities conducted worldwide, particularly narcotics-trafficking and corruption. Switzerland's extensive market in fine arts is also used to launder money. 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. For example, some of the money generated by Albanian narcotics-trafficking rings in Switzerland goes to armed Albanian extremists in the Balkans.

Switzerland ranks fifth in the highly profitable artwork trading market. It exported \$877 million worth of artwork worldwide in 2003, and another \$786 million from January to October 2004. Generating about \$951 billion a year in turnover, the Swiss market offers lucrative opportunities for organized crime to transfer stolen art or to use art to launder criminal funds. The United States is by far Switzerland's most important trading partner, and purchased \$442 million of "Swiss" works of art in 2003, and \$332 million from January to October 2004. Because art works, which may have been smuggled into Switzerland, can legally be re-exported as genuine Swiss artwork after five years, the Swiss art market is especially attractive for unethical transactions.

Switzerland has duty free zones. The Customs authorities supervise the admission into and the removal from customs warehouses. Warehoused goods may only undergo manipulations necessary for their maintenance, or 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, etc. all apply. In view of the fact that Customs may and frequently does 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.

In December 2001, the Swiss Federal Council (Cabinet) agreed to consider expanding the scope of the 1998 federal anti-money laundering (AML) law to include art and jewelry dealers. The revised AML bill will be discussed in January 2005 in the context of the Financial Action Task Force (FATF) Forty Recommendations. In the meantime, AML regulations have been extended to cover art dealers to the extent that they are acting specifically as "financial intermediaries" between a seller and a buyer.

Additionally, on June 17, 2003, the parliament adopted a bill on the transfer of cultural goods, which regulates the return of looted cultural objects. The new legislation, which is expected to come into force by April 2005, extends the timeframe from the current five years to meet the UN International Standards of 30 years, as defined in the 1970 UNESCO Convention. It also will enable police forces to search bonded warehouses and art galleries.

Money laundering is a criminal offense. Switzerland has significant AML legislation in place, making banks and other financial intermediaries subject to strict know your customer and reporting requirements. 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.

The current money laundering laws and regulations have been extended to non-bank financial institutions. Consequently, all non-bank financial intermediaries are required to either join an accredited self-regulatory organization (SRO), or come under the direct supervision of the Money Laundering Control Authority (MLCA) of the Federal Finance Department. The MLCA was formed in 1998 to oversee anti-money laundering laws in the non-banking sector. The SROs must be independent of the management of the intermediaries they supervise and must enforce compliance with due diligence obligations. Noncompliance can result in a fine or a revoked license. About 7,000 fiduciaries operate in this previously unregulated arena. The MLCA has shown willingness to take action against financial intermediaries: in 2003, the MLCA ordered the official liquidation of five financial intermediaries and the removal from the commercial register of two others, because they failed to comply with AML regulations. Reporting regulations on international money transactions, applicable to money transmitters in particular, have been tightened as well.

In December 2002, the new money laundering ordinances of the Swiss Federal Banking Commission were adopted; these became effective on July 1, 2003. These new 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 (KYC) 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 changes also require increased due diligence in the cases of politically exposed persons by ensuring that decisions to commence relationships with such persons be undertaken by the senior executive body of a firm. Additionally, the ordinance mandates computer-based transaction monitoring systems for all but the smallest financial intermediaries. All cross-border wire transfers must contain details about the funds remitters. The provisions of the ordinance also address Swiss supervision of subsidiaries belonging to a consolidated group of financial intermediaries (for which information channels must be established). All provisions apply to correspondent banking relationships as well. Shell banks-banks with no physical presence at their place of incorporation-may not maintain any correspondent bank accounts.

In October 2003, the Swiss Cabinet mandated an interdepartmental working group led by the Ministry of Finance to review Switzerland's compliance with the revised FATF Forty Recommendations. In December 2003, the MLCA effected a new money laundering ordinance which implements the revised Recommendations. The FATF is expected to review implementation by early 2005.

In July 2003, the government-sponsored Zimmerli Commission, charged by the Finance Ministry with examining reform of finance market regulators, presented 46 recommendations. Most notably, the Committee recommended merging the Federal Banking Commission and the Federal Office for Private Insurance, or the banking and insurance sectors, into a single, integrated financial market supervision body, to be known as FINMA. In November 2004, the Cabinet instructed the Finance Ministry to draft a parliamentary bill providing for the establishment of the FINMA. Under the Cabinet's proposal, the MLCA would also be included within the FINMA. The draft bill is scheduled for submission to Parliament by the end of 2005. The proposed changes are extremely far-reaching

In June 2004, the Cabinet submitted draft legislation to Parliament on auditing reform. The draft revision more tightly delineates the duties of auditing firms of large corporations and strengthens provisions on auditors' independence to prevent conflicts of interest. The draft legislation also provides for a public monitoring body of auditors to ensure that only sufficiently qualified experts perform auditing services.

Switzerland's banking industry offers the same account services for both residents and nonresidents. These can be opened through various intermediaries who advertise their services. As part of Switzerland's international financial services, 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.

The 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.

Swiss casino operators have joined counterparts from Greece, Austria, Finland, Spain, Portugal, and the United Kingdom to form a new Casino Operators' Association. Among the stated priorities for the group are addressing anti-money laundering issues and responsible gaming practices.

The Money Laundering Reporting Office Switzerland (MROS) is Switzerland's Financial Intelligence Unit (FIU). All financial intermediaries (banks, insurers, fund managers, currency exchange houses, securities brokers, etc.) are legally obliged to establish customer identity when forming a business relationship. They also must notify the MROS, or a government authorized supervisory body, if a transaction appears suspicious. In March 2004, MROS released figures for the previous year: In 2003, money laundering cases rose 32 percent over 2002 figures, with more than 860 reports of suspicious transactions (STRs) worth approximately \$460 million. As in 2002, the majority of reports came from the non-banking sector, probably due to the stricter reporting regulations directed at non-banking financial intermediaries. However, while the percentage of STRs coming from banks has decreased, the actual number of STRs from the banks has continued to increase.

The Government of Switzerland has made it a key foreign policy goal to correct the country's image as a haven for illicit banking services. The Swiss believe that their system of self-regulation, which incorporates a "culture of cooperation" between regulators and banks, equals or exceeds that of other countries. The primary interest of the Swiss system is to avert bad risks by countering them at the account-opening phase, where due diligence and KYC address the issues, rather than relying on an early-warning system on all filed transactions. The Convention on Due Diligence is very comprehensive, requiring the identification of the client and the beneficial owner, who needs to be a physical person. Because of the due diligence approach the Swiss have taken, there are fewer STRs filed than in other countries, but the ones that are filed lead to the opening of criminal investigations 75 percent of the time. In January 2003, Switzerland won a battle when the European Union backed away from demands that Switzerland scrap banking secrecy. Despite the measures that Switzerland has taken, it is likely to endure more criticism from other countries for its continued banking secrecy laws and its refusal to look upon tax evasion as a crime.

The banking community cooperates with enforcement efforts. The Oversight Commission of the Swiss Bankers Association fined Credit Suisse for inadequate due diligence in connection with a total of \$214 million deposited in the bank by former Nigerian dictator Sani Abacha. Swiss press reports put the fine at \$500,000 (SFr. 750,000 at the time), making it the largest fine ever imposed by the Commission. The recipient of the fine will be the International Red Cross Committee, a Swiss organization.

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. Formerly, the individual cantons were charged with investigating money laundering offenses on their own. 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, and 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. Under Swiss law, suspect assets may be frozen for up to five days while a prosecutor investigates the suspicious activity. Switzerland

cooperates with the United States to trace and seize assets, and has shared 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.

In addition, legislation permits "spontaneous transmittal"-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. On March 31, 2003, the Swiss Federal Court rejected an appeal by Raul Salinas, brother of a former president of Mexico and main suspect in a major money laundering affair, to release millions of dollars blocked on 10 different Swiss bank accounts. In December 2004, Swiss judicial authorities handed over to Argentinean authorities banking information, in the context of criminal investigations, against former Defense Minister Oscar Camilion and former Air Force chief Juan Paulik. Camilion was forced to resign in June 1996.

During 2002, the Swiss Federal Council presented a bill to the Nationalrat, Switzerland's lower house, that addresses a number of terrorism issues surrounding ratification of the UN terrorism conventions. This bill includes a provision on terrorist financing that introduces criminal liability for legal persons involved in terrorism financing. The Swiss House was scheduled to consider it in the first half of 2003. The amended Swiss penal code makes terrorism financing a predicate offense for money laundering. Changes in the Criminal Code in 2003 also make terrorism financing a predicate offense in money laundering, and expand the scope of application to legal persons.

The ordinances adopted in December 2002 also include new rules against terrorism financing, stating that instruments currently used to prevent money laundering are also applicable to the prevention of terrorism financing; if a financial intermediary investigates the background of an unusual or suspicious transaction, and linkages with a terrorist organization are revealed, the institution must report the matter to the FIU immediately.

Since September 11, 2001, Swiss authorities have been alerting Swiss banks and non-bank 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 assets of organizations and individuals designated by the UNSCR 1267 Sanctions Committee. In the 2003 reporting period, MROS received reports of five cases possibly linked to the funding of terrorism. The total amount of money involved was \$115,000. All the reports involved individuals and institutions appearing on the USG lists. The five reports were transmitted to the Swiss Attorney General in Berne.

Along with USG 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 Ladin and al-Qaida under UN resolutions. The Swiss Attorney General also separately froze 41 accounts representing about \$25 million, on the grounds that they were related to terrorism financing, but the extent to which these funds overlap with the UN lists has yet to be determined. In January 2003, the Swiss Ministry of Justice handed over banking information to U.S. authorities, following a legal assistance request issued in April 2002. The request related to a bank transfer of \$1.4 million, addressed to the Benevolence International Foundation, a Chicago-based Islamic foundation designated as a terrorist financier. The transfer originated from a Swiss bank account whose account holder was a company located in the Virgin Islands. The firm had initially lodged a complaint against this decision to the supreme Swiss federal court but was turned down in November 2002.

Switzerland has ratified the Council of Europe (COE) 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 has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. To date, Switzerland has not ratified the 1988 UN Drug Convention.

Swiss authorities cooperate with counterpart bodies from other countries. Requests for cooperation with Liechtenstein, Switzerland's closest neighbor both culturally and geographically, have tripled. 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 supervisory purposes. The U.S.-Swiss extradition treaty permits extradition for any unlawful act punishable by imprisonment in both countries. Switzerland is a member of the FATF, the Egmont Group and the Basel Committee on Banking Supervision.

The Government of Switzerland should extend its anti-money laundering program to include dealers in high-end goods. Switzerland can also continue to improve on its anti-money laundering regime, as it has been doing, and address deficiencies that it finds, as well as continuing to work toward full implementation of its anti-money laundering/counterterrorist financing regime.

## **Syria**

Due to its relatively undeveloped banking sector, Syria is not a likely center for money laundering via the formal financial sector. From the time that private banks were nationalized in the early 1960s, and prior to last year, Syria's entire financial system was owned and operated by the state. However, in January 2004, private banks began operating in Syria. Currently three private banks are open for business. The existing public banks remain inefficient and highly regulated, and focus almost exclusively on financing public enterprises. Until late 2004, several foreign banks had been operating in Syrian duty-free zones without direct supervision by the Government of Syria (SARG). The SARG, however, recently began applying banking controls and regulatory oversight to these banks.

The U.S. Department of State designated Syria as a State Sponsor of Terrorism in 1979. In May 2004, the U.S. Department of the Treasury designated the Commercial Bank of Syria (CBS), along with its subsidiary, the Syrian Lebanese Commercial Bank, as a financial institution of "primary money laundering concern," pursuant to Section 311 of the USA Patriot Act. This designation remains in place, but the final rulemaking on the implementation of the special measure against CBS has not been issued, pending further discussions between the U.S. Government and the Government of Syria (SARG). In September 2004, U.S. and Syrian officials met to discuss deficiencies in SARG banking regulations. The U.S. Government later suggested remedial actions that Syria could take to conform to international banking standards, particularly those outlined in the recommendations of the Financial Action Task Force (FATF).

The Government of Syria strictly controls foreign currency flows out of the country, contributing to the use of alternative and "informal" systems of moving money or transferring value. Syrian businessmen usually depend on banks in neighboring Lebanon and Jordan to transact a full range of banking services. The private sector routinely uses foreign currency to finance imports, generally by using letters of credit from Lebanon and Europe. Due to foreign exchange controls, the private sector also has restricted access to foreign currency. Illicit proceeds from the narcotics trade may flow through Syria, but they are usually moved to Lebanon for laundering purposes. As a result, the primary money laundering vulnerability in Syria is not necessarily through financial institutions but through alternative remittance systems such as hawala, trade-based money laundering, and currency smuggling. Such money laundering methodologies are often used to finance terrorism throughout the region and elsewhere. The opening of private banks is a positive development in terms of modernization of Syria's financial sector, but at the same time it makes the banking system increasingly vulnerable to money laundering, at least until such time as the SARG completes the implementation of measures to facilitate its oversight of financial transactions.

Due to a distrust of public banks, strict currency restrictions, and displeasure with the official exchange rate, most Syrians prefer to utilize informal banking systems to transfer currency into, around, and out of Syria, sometimes by physically moving cash via Syrian bus and shipping companies with offices in the region. Relatives, friends and colleagues often provide a similar service using foreign bank accounts, particularly in Lebanon. In instances where no relative or friend is available and/or the amount to be transferred is too high, a few money changers, well known to the business community and operating with tacit SARG approval, also provide a means of depositing hard currency in overseas accounts. These mechanisms are a form of hawala.

The government-controlled banking system in Syria consists of the Central Bank of Syria and five public banks, each specializing in one aspect of economic activity: the Commercial Bank of Syria, the Agricultural Cooperative Bank, the Industrial Bank, the Real Estate Bank, and the People's Credit Bank. These banks have in the past employed a rigid interest rate structure that discourages savings deposits, particularly during periods of inflation. Until January 2004, when the first private banks opened, only the Commercial Bank of Syria was been permitted to provide commercial banking services. As the sole legal trader of foreign currencies, the Commercial Bank also effectively controlled all legal foreign trade and all foreign currency transactions.

In addition to monopolizing the exchange of foreign currencies, the SARG maintains one of the last remaining fixed, multiple exchange rate systems in the world, employing different rates depending on the nature of the transaction. There are reports that the SARG may take steps toward eliminating the multiple exchange rate system in 2005. Until it is changed, however, this inefficient system contributes to the use of alternative methods of transferring value outside the state-controlled banking system. There are reports that such transactions occur with the tacit approval, if not involvement, of SARG officials. A large percentage of Lebanon's banking services involve Syrian accounts.

In April 2001, Law No. 28 legalized private banking. That same month, Law No. 29 established rules on bank secrecy. The first private banks opened in January 2004, but the services they provide are limited under current governmental regulations. Much still needs to be done to fundamentally restructure the banking sector, particularly in terms of either suspending or amending existing regulations that prohibit the three established private banks from operating fully. The SARG continues to work on detailed regulations that will govern the operation of private banks. These private banks must have a 51 percent Syrian ownership (individual or consortium), while non-Syrian banks interested in investing in this new financial sector often finance the other 49 percent.

In September 2003, Syria passed Legislative Decree No. 59, criminalizing money laundering and creating an Anti-Money Laundering Commission. While this was an important movement in principle toward addressing vulnerabilities in the banking sector, particularly the new vulnerabilities arising from the opening of private banks, it is not yet clear what relationship the commission will have with financial institutions or whether the commission will hold effective investigative powers. In December 2004, the SARG prohibited private bank representation on the Anti-Money Laundering Commission, in order to ease conflict-of-interest concerns.

Syria is a party to the 1988 UN Drug Convention. It is also in the process of becoming a party to the UN International Convention for the Suppression of the Financing of Terrorism. It signed the UN Convention against Transnational Organized Crime (in 2000), but has not yet ratified it. Syria is a charter member of the Middle East and North Africa Financial Action Task Force (MENAFATF) that was inaugurated in Bahrain in November 2004. The MENAFATF is a FATF-style regional body. The creation of the MENAFATF is critical for pushing the region to improve the transparency and regulatory frameworks of its financial sectors.

The Government of Syria should immediately stop all support of terrorist organizations. It should continue to implement comprehensive anti-money laundering and counterterrorism finance legislation that adheres to international standards, including the creation of an independent Financial Intelligence Unit (FIU). Syria should then take meaningful steps to enforce the law and follow-up rules and regulations governing the banking sector. Syria should ratify both the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime.

## **Taiwan**

Taiwan's modern financial sector and its role as a hub for international trade make it attractive to money laundering. Its location astride international shipping lanes makes it vulnerable to transnational crimes such as narcotics-trafficking and smuggling. The use of alternative remittance systems or "underground banking" is a money laundering vulnerability. There is a significant volume of informal financial activity through unregulated non-bank channels. According to suspicious activity reports (SARs) filed by financial institutions on Taiwan, the predicate crimes linked to SARs include financial crimes, corruption, narcotics, and other general crimes, in that order.

Taiwan's anti-money laundering legislation is embodied in the Money Laundering Control Act (MLCA) of April 23, 1997. 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).

The Legislative Yuan 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 of significant currency transactions of over New Taiwan (NT)\$1 million (approximately \$30,000) to the MLPC. 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. Also as a result of the 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.

The time limit for reporting cash transactions of over NT\$1 million is within five business days. Banks were also barred from informing customers that a suspicious transaction report had been filed. In addition, two new articles were added to the MLCA, granting prosecutors and judges the power to freeze assets related to suspicious transactions, and giving law enforcement more powers related to asset forfeiture and the sharing of confiscated assets. 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. Reports of suspicious transactions must be submitted to the MLPC within 10 business days after the transaction took place.

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 MLPC to access all relevant financial account information. Financial institutions are held responsible if they do not report suspicious transactions. In May 2004, the Ministry of Finance also required banks to demand two types of identification and to keep copies 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 NT\$200,000-1 million (\$6,000-30,000) for not following the MLCA.

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 (BOMA), and MLPC. These supervisory agencies conduct background checks on applicants for banking and business licenses. Offshore casinos and Internet gambling sites are illegal.

From January to September 2004, Taiwan investigated 505 cases of possible money laundering. Among these cases, 442 were economic crimes, seven involved government corruption, and seven were narcotics-related crimes. Total money laundering during this period amounted to NT\$1.244 billion (about \$38 million). Of the 505 cases investigated, 287 involved money laundering via bank transactions, 213 involved postal remittances and savings banks, and one case involved a credit union.

Individuals are required to report currency transported into or out of Taiwan in excess of NT\$60,000 (approximately \$1,765), \$5,000, or \$5,000 worth of foreign currency. Starting in March 2004, over 6,000 Chinese renminbi (\$725) must also be reported. When foreign currency in excess of NT\$500,000 (approximately \$14,700) 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.

Starting in September 2003, the Directorate General of Customs was responsible 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 NT\$1.5 million. Among the 542 cases reported between

September 2003 and June 2004, the center said it had found several cases that might involve illegal underground banking activities, and these were under investigation.

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 January 2005 it is still pending legislative approval. 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 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 UNSCR 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. In accordance with UN Security Council Resolution 1373, the MLCA was amended to allow the freezing of accounts suspected of being linked to terrorism. Identified to date. In 2004, there was one suspected terrorist finance case reported. Subsequent investigation determined that the suspect was not a terrorist or a financier of terrorism.

Alternative remittance systems, or underground banks, are considered to be operating in violation of Banking Law Article 29. Authorities on 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 on 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 already required to register with the government.

Taiwan's only free trade zone began operation in Keelung on October 1, 2004. Entities wanting to operate in the free trade zones must submit applications to the port authorities. Entities can conduct simple processing of commodities in the zone and re-export them without inspection by customs. There is no indication that the zone is used in money laundering schemes or by financiers of terrorism. Keelung port authority has a panel composed of members from various enforcement agencies to conduct checks of commodities, transportation, and accounting. According to Taiwan's Banking Law and Securities Trading Law, in order for financial institutions to conduct foreign currency operations, Taiwan's Central Bank must first approve the institution to for this function. The financial institutions must then submit an application to port authorities to establish an offshore banking unit in the free-trade zone.

Taiwan has established drug-related asset seizure and forfeiture regulations, which state that according to treaties or agreements, Taiwan's Ministry of Justice shall share seized assets with foreign official agencies, private institutions or international parties which 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 January-September 2004, total seized assets reached NT\$20 million (about \$660,000).

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 territories 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 on 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 actively participates in the Group's meetings. The MLPC is a member of the Egmont Group. In 2003, thirty-six information exchanges took place between Taiwan and international counterparts, including the United States, related to money laundering investigations.

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 that would promulgate regulations regarding alternate remittance systems.

## **Tajikistan**

Tajikistan is not a major financial center in the region and does not have a developed banking system. Prosecutions for financial criminal activity are unusual, although the ringleaders of the Ponzi bead-scheme that defrauded hundreds of people out of tens of thousands of dollars in 2003 were convicted in 2004 and sentenced to terms ranging from eight to twenty years. Tajikistan is not an offshore center, but offshore zones are often used while concluding deals with foreign enterprises. Foreign banks operate in the country, including an Iranian bank.

Domestic goods smuggling is a concern in Tajikistan. Consumer goods, mostly apparel and low-cost household appliances, are smuggled to avoid customs duties and local taxes. In most cases, goods such as tobacco, alcohol, and fuel are not "officially" imported to Tajikistan. For example, a shipment transiting Tajikistan intended for Kazakhstan or Afghanistan never reaches the destination country. While there is certainly a market for smuggled goods, there is little evidence that most items are financed with narcotics money, with the exception of imported cars and other luxury items.

The Tajik Criminal Code of May 21, 1998, Art. 574-Legalization (laundering) of Illegally Obtained Income prohibits money laundering. This prohibition includes not only narcotics money laundering, but also circumvention of other financial currency controls (for example, removal of currency into the offshore zone, unlawful usage of a charity, insurance companies, etc.).

The Law on Banking Activity of May 23, 1998 (No.648 AMOPT NO. 10, 1998)-Art. 32 addresses banking secrecy laws that prevent disclosure of client and ownership information to bank supervisors and law enforcement authorities for domestic and offshore financial services companies. While the Government of Tajikistan (GOT) has not yet addressed the problem of international transportation of illegally sourced currency and monetary instruments, and has a long way to go to meet "due diligence" standards, it has instituted cross-border currency reporting requirements. Travelers may depart with a maximum amount of \$2,000 without any certifying document. When amounts exceed \$2,000, an authorized exchange office issues a certificate of transaction for purchase of currency (USD), a.k.a.

"form 377," and then the head office (bank) issues a "Ruhsatnoma"—permission to take the cash out of the country. Travelers may enter Tajikistan with unlimited quantities.

Banks are not required to know, record, or report the identity of customers engaging in significant transactions unless criminal proceedings have been undertaken against a specific individual or organization. Some civil proceedings can also trigger this scrutiny. For example, in civil or administrative proceedings, a court can request information about accounts or the nature and value of property kept in bank safes, or request information which is considered to be a "bank secret" in cases when the bank's client represents one of the sides in the proceedings, if asset forfeiture can be applied, or in inheritance cases. Banks and other financial institutions also are not required to maintain records to reconstruct activity. Financial institutions make no regular reports of transactions or other activity, and reporting officers have no special legal protections with respect to cooperating with law enforcement. There is no legal mechanism to insure law enforcement's access to the information related to illegal financial operations.

Money laundering controls are applied to all financial institutions, including exchange offices, brokerages, etc., that are licensed by the National Bank and subject to the same laws as banks. There have been no arrests or prosecutions for money laundering or terrorist financing since January 1, 2002.

Although negotiations are underway for developing an asset seizure program, the GOT does not currently have any asset-seizure mechanisms. The main barriers to implementing such a program are corruption and the underdeveloped legal system. The GOT passed Criminal Code, Art. 57, stating that asset forfeiture is possible but also specified exceptions. A program is being developed to allow the Drug Control Agency to use this law as one means of achieving self-sustainability.

The Tajiks used asset forfeiture procedures in the case of former Commander of the Presidential Guard General Gaffor Mirzoev, who was arrested in August this year and charged with a number of crimes: illegal storage of weapons, murder, illegal commercial activity, illegal appropriation of state property and its use for personal benefit. In November, the Supreme Economic Court passed a resolution to transfer Dushanbe Meat Processing Plant, Entertainment Complex "Jomi Jamshed," and the shop "Kooperator" located in Kulyob from Mirzoev's Company "Mirzoi Rahmon" to the jurisdiction of the Tajik State Committee for Management of State-owned Property, after the Prosecutor General's Office established that these entities had been privatized illegally.

The GOT has criminalized terrorist financing, as covered by the above-mentioned general money laundering statute. Terrorist finance is considered to be a "serious crime." There were no reported cases of suspected terrorist assets being frozen in 2004 because no known terrorist assets were discovered.

Several laws have been adopted, e.g.: Civil Code, Art. 284—Illegal Transactions with Precious Metals, Gems and Gold—to address the misuse of gold, precious metals and gems. The GOT has not addressed alternative remittance systems. Remittances from labor migrants are mainly from Russia and other NIS countries, and are seasonal. The GOT has waived a 30 percent fee on bank transfers, making remittances sent via banks more effective.

Tajikistan and the U.S. Government have not yet reached an agreement for a mechanism for exchanging adequate records in connection with investigations and proceedings relating to narcotics, terrorism, terrorist financing and other serious criminal investigations, and no negotiations are currently underway. However, the U.S. Government regularly sends information regarding designated individuals and organizations subject to asset forfeiture to the Tajik Ministry of Foreign Affairs (MFA). The MFA distributes this information to the Ministries of Security, Finance, and Interior, and other governmental structures, which conduct appropriate checks. The GOT has not adopted laws or regulations that ensure the availability of adequate records in connection with narcotics, terrorism, terrorist financing or other investigations. Two GOT officials participated in the Roundtable Conference on legislative reforms to combat money laundering and terrorist financing, in Tashkent, Uzbekistan, in July 2004.

Despite a primitive banking system and the use of a barter system in many rural areas, Tajikistan signed the CIS Agreement on the Legal Assistance and Cooperation on Civil, Family and Criminal Cases of January 22, 1993, and is a member of the CIS Counterterrorism Center. The GOT signed the UN International Convention for the Suppression of the Financing of Terrorism in November 2001, but has not yet ratified it. Tajikistan is a party to the UN Convention against Transnational Organized Crime and a charter member of the new Eurasian Group on Combating Money Laundering and Financing of Terrorism, a FATF Style Regional Body established in October 2004.

The Government of Tajikistan should enact and implement anti-money laundering and counterterrorist financing legislation that comports with international standards. Additionally, mechanisms to share information among financial institutions, regulatory authorities and law enforcement entities should be developed to promote the successful prosecution of financial crime cases. Tajikistan should ratify the UN International Convention for the Suppression of the Financing of Terrorism.

## **Tanzania**

Tanzania is not considered an important regional financial center, but is vulnerable to money laundering because of the weaknesses of its financial institutions and law enforcement capabilities. A weak financial sector and an under-trained, under-funded law enforcement apparatus make such crimes difficult to track and prosecute. Officials have noted that some real estate and used car businesses are used for money laundering purposes. Government officials have also cited the emerging casino industry as an area of concern for money laundering. Money laundering is more likely to occur in the informal non-bank financial sector, as the formal sector is still relatively undeveloped. The prevalence of hawala and the threat of terrorist organizations on the unregulated island of Zanzibar make Zanzibar an area of concern. Officials indicate that money laundering schemes in Zanzibar generally take the form of foreign investment in the tourist industry and bulk cash smuggling. The most likely sources of illicit funds include Asia and the Middle East, and to a lesser extent Europe. Such transactions rarely include significant amounts of U.S. currency.

The Proceeds of Crime Act of 1991 criminalizes narcotics-related money laundering. However, the Act does not adequately define money laundering, and it has only been used to prosecute corruption cases. The law obliges financial institutions to maintain records of financial transactions exceeding 100,000 shillings (approximately \$109) for a period of 10 years. If the 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 not required. The Central Bank has issued regulations requiring financial institutions to file suspicious transaction reports (STRs), but this requirement is not being enforced, and no mechanism exists for receiving and analyzing the STRs. Financial institution employees are legally protected from liability stemming from reporting suspicious transactions. Current law does not hold financial institutions responsible if they are found to have been used to launder money.

The 2002 Prevention of Terrorism Act criminalizes terrorist financing. It also requires all financial institutions to inform the government each quarter as to whether any of their assets or transactions may be associated with a terrorist group, although the implementing regulations for this provision have not yet been drafted. Under the Act, the government may seize assets associated with terrorist groups. The Bank of Tanzania (the Central Bank) circulates to Tanzanian financial institutions the list of individuals and entities on the UNSCR 1267 Sanction Committee's consolidated list, but to date no assets have been frozen under this provision. The Government of Tanzania (GOT) did take action in 2004 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 United States in investigating and combating terrorism. Tanzanian officials have consistently cooperated in the exchange of counterterrorism information with U.S. authorities.

The GOT became a party to the UN International Convention for the Suppression of the Financing of Terrorism in 2003. Tanzania is a party to the 1988 UN Drug Convention and has signed the UN Convention against Transnational Organized Crime. Tanzania is a member of the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG), which was founded in 1999. The GOT continues to play a leading role in the operation of this FATF-style regional body and has detailed

personnel to the ESAAMLG Secretariat, located in donated office space in Dar es Salaam. Tanzania also continues to host the ESAAMLG task force meetings held each March.

In line with Tanzania's commitment to supporting the ESAAMLG, Tanzania has created a multi-disciplinary committee on money laundering and a drafting committee that has prepared new anti-money laundering legislation. A Tanzanian Ministry of Finance official stated in August 2004 that the drafting committee was in the process of receiving comments on the language of its bill from stakeholders, and that the bill would likely be presented to the Parliament in January 2005. The proposed legislation provides for the creation of a Financial Intelligence Unit (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.

The Government of Tanzania should maintain the momentum towards enacting its anti-money laundering law. It should continue to work through Southern African Anti-Money Laundering Group (ESAAMLG) to establish a Financial Intelligence Unit (FIU) and develop a comprehensive anti-money laundering regime that comports with international standards.

## **Thailand**

Thailand is vulnerable to money laundering as a result of a significant underground economy and cross-border crime problems with illicit narcotics, contraband, and smuggling. Thailand continues to remain vulnerable to money launderers. Money laundering occurs in both the banking and non-banking systems. Over the last decade, there has been a considerable decrease in the amount of heroin produced in the Golden Triangle region of Burma, Laos, and Thailand. However, drug traffickers still use Thailand's banking system to hide and move their proceeds. It is a key destination, transit and source country for organized international migrant smuggling and trafficking in persons. Thailand is a major production and distribution center for counterfeit goods of all types, including the production and sale of fraudulent travel documents. The underground banking system is widely used for money laundering. Illegal gambling, prostitution, and underground lotteries are a significant part of Thailand's sizeable underground economy. There is a black market for smuggled goods for the purpose of evading customs duties. With the acceleration in economic growth, tax evasion has reportedly increased, and significant financial and securities fraud has been reported. Public sector corruption, particularly in criminal justice institutions, remains a major problem. Thailand experienced an increase in financial crimes in 2004.

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, and blackmail. It also provided for the establishment of an Anti-Money Laundering Office (AMLO). 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 over 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 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, as provided in Recommendations 1 and 2 of the Forty Recommendations of the Financial Action Task Force (June 2003), 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.

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) that cooperate with law enforcement entities are protected. Thailand does not have secrecy laws that prevent disclosure of

client and ownership information of bank accounts to supervisors and law enforcement authorities. The AMLA gives the anti-money laundering office the authority to compel a financial institution to disclose such information.

In early 2004, the Thai cabinet approved amendments to the AMLA to create an asset forfeiture fund, authorize asset sharing, and add the following additional predicate offenses: weapons smuggling, illegal gambling, government procurement fraud, crimes affecting natural resources and the environment, intellectual property rights infringement, and Money Exchange Control Act violations. These amendments have been under consideration by the Council of State and are expected to be submitted to the Parliament in early 2005. Active consideration is being given to adding eight additional predicate offenses to the anti-money laundering statute, to include offenses related to natural resources, currency exchange, stock market manipulation, gambling, firearms, conspiracy in awarding government contracts, labor fraud, and tax evasion. Since October 27, 2000, there have been 68 convictions under the AMLA. Cases are proceeding for civil forfeiture against property involved in drug trafficking, prostitution, public fraud and embezzlement, customs evasion, and corruption offenses.

The Bank of Thailand regulates financial institutions in Thailand, but 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 and had hoped to begin such examinations in 2004. The BOT has now agreed that AMLO should be responsible for on and off site audits for AMLA compliance. The target date for such examinations has now slipped to early 2005.

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 two million baht (approximately \$52,000), and property transactions exceeding five million baht (approximately \$130,000), have been in place since October 2000. However, AMLO has been considering a proposal to lower the threshold for reporting cash transactions to 400,000 baht (\$10,500). The proposal is not yet in effect and the likelihood of its adoption is in doubt, since (in early February 2005) the Prime Minister publicly expressed his opposition to it. The AMLO is also drafting amendments requiring gold and jewelry shop owners and used car dealers to report transactions over 400,000 baht (\$10,500), and is consulting with private industry, but those amendments have also been opposed by affected industries as too cumbersome and unnecessary, and are under review by the Prime Minister.

The various land offices are also required to report on any transaction involving property of five million baht or greater, or a cash payment of two million baht or greater, for the purchase of real property. 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) 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.

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. Thailand's 44 BIBFs are now subject to the AMLA.

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). Within the Asia Pacific Economic Council (APEC), Thailand is working with several other countries on a study of alternative remittance systems. Moneychangers frequently act as illegal remittance agents. Remittance agents, including informal remittance businesses, require a license from the Ministry of Finance. Operating a money transfer business also requires a license. The Ministry of Finance issued the Notification to Authorized Persons on July 30, 2004, and to Money Transfer Agents August 4, 2004. The Bank of Thailand issued a Notice to the Competent Officer on the Procedures and Guidelines to operate as Authorized Persons dated August 6, 2004, and to Money Transfer Agent dated August 6, 2004. These new guidelines of BOT and MOF became effective on August 11, 2004. 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 applicants criminal history and AML record. Licensed agents are also subject to monthly transaction reporting and a 3-year record maintenance requirement. At present, there are about 270 authorized moneychangers and five remittance agents. There is no limitation on the amount of foreign currency that a person can take in or out of Thailand. A customer can transfer an unlimited amount of money through a commercial bank, with the required supporting documentation. At present, moneychangers have to report financial transactions to the Anti-Money Laundering Office (AMLO), while remittance agents do not. As part of the August 6, 2004 notice, the Bank of Thailand limited the annual transaction volume for agents to \$60,000 for offices in the Bangkok area and \$30,000 for offices located in other areas.

The 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. With respect to charities, The Bank of Thailand (BOT) does not have regulation that gives it explicit authorization to control charitable donations. However, the BOT is working with the Anti-Money Laundering Office to monitor these transactions under the Exchange Control Act of 1942.

The AMLA created the Anti-Money Laundering Office (AMLO), which became fully operational in 2001. AMLO is Thailand's Financial Intelligence Unit (FIU). When first established, AMLO reported directly to the Prime Minister. In October 2002, a reorganization of the executive branch took place, and AMLO was designated as an independent agency under the Ministry of Justice. AMLO receives, analyzes, and processes suspicious and large transaction reports, as required by the AMLA. From January through September 2003, the AMLO received 636,129 currency transaction reports and 84,967 suspicious transaction reports.

In addition, the AMLO is responsible for investigating money laundering cases for civil forfeiture purposes and for the custody, management, and disposal of seized and forfeited property. The AMLO is also tasked with providing training to the public and private sectors concerning the provisions of 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. From October 2003 to October 2004, AMLO filed 362 cases of civil asset forfeiture involving assets worth 3.771 billion baht. Of these, forfeiture judgments have been entered in 152 cases involving 418 million baht. In pursuing its civil forfeiture investigations, AMLO has received valuable cooperation from financial institutions, particularly the commercial banks.

In 2004, the Prime Minister's "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 can receive personal payments from the property they seize in money laundering cases. The system that Thailand has created undermines the integrity of its AML regime and may impede international cooperation. After domestic and international criticism of this system, the Ministry of Justice is considering alternatives to personal commissions from seizures, including the creation of a forfeiture fund for the forfeited proceeds to be dedicated to various programs, rather than personal purposes.

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 (\$4 million) and 1,644 cases are on trial. Two hundred million baht (\$5,000,000) have been confiscated and sent to the Narcotics Control Fund.

As part of a general reorganization of the Executive Branch, the Thai Parliament has authorized the establishment in the Ministry of Justice of a new criminal investigative agency, the Department of Special Investigations (DSI), separate from the Royal Thai Police Office. On November 24, 2003, Parliament approved legislation defining DSI's organization, authorities, and responsibilities. The latter include 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, now including terrorism. The DSI, AMLO, and the Royal Thai police all have the authority to identify, freeze, and/or forfeit terrorist finance- related assets.

Thailand is a party to the 1988 UN Drug Convention. In September 2004, Thailand became a party to 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) the UN Convention against Corruption. In April 2005, Thailand will host the 11th United Nations Crime Congress, which will emphasize counterterrorism as one of its principal themes. The RTG has issued instructions to all authorities to comply with UNSCR 1267, including the freezing of funds or financial resources belonging to the Taliban and the al-Qaida network. To date, Thailand has not identified, frozen, and/or seized any assets linked to individuals or entities included on the UNSCR 1267 Sanctions Committee consolidated list. However, AMLO has identified some suspicious transaction reports derived from financial institutions and has initiated cases that may involve terrorist activities using non-governmental or non-profit organizations as a front. Thailand has a Mutual Legal Assistance Treaty (MLAT) with a number of countries, including the United States. It has a memorandum of understanding on law enforcement issues with an additional number of other countries. 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 BOT and AMLO have agreed that AMLO will be responsible for both offsite and onsite supervision of banks to ensure that Financial Institutions comply 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. It is therefore important that BOT/AMLO compliance examinations begin early in 2005 and that other relevant agencies (SET, DOI, and CPD) be working with AMLO to establish policies and procedures for supervisory oversight of AML/CFT compliance. 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 to further strengthen its anti-money laundering regime against crime, particularly by expanding its list of predicate offenses to include a broader base of serious financial crimes, such as arms/weapons trafficking, alien smuggling, and environmental crimes, as well as making the "structuring" of transactions a criminal offense. It should extend the law to cover instrumentalities. Thailand should ratify the UN Convention against Transnational Organized Crime. Thailand should also immediately rescind its new rewards program for AMLO investigators who seize assets under the anti-money laundering laws, and for agents of other agencies that engage in such practices, 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.

## **Togo**

Togo's poor financial infrastructure makes it an unlikely venue for money laundering through its financial institutions. Its porous borders, however, make it a transshipment point in the regional and sub-regional trade in narcotics. Togo's 1998 drug law criminalizes narcotics-related money laundering and penalizes offenses with up to 20 years in prison. However, there have never been any arrests for

money laundering. Financial institutions are required to monitor and report monetary transactions above a threshold appropriate to the local economic situation, and must maintain records of such transactions and supply them to government authorities on request. Financial institutions are legally protected in respect to their cooperation with law enforcement authorities. Due diligence legislation applies to bankers and other professionals, although no arrests have been made for violations of this law.

The Government of Togo (GOT) has the legal authority to seize assets associated with narcotics-trafficking. In 2001, President Eyadema created the national Anti-Corruption Commission to combat corruption and money laundering.

Terrorist financing is not a criminal offense in Togo, although draft legislation is pending. The GOT has circulated to Togolese financial institutions the names of suspected terrorists and terrorist organizations listed on the UN 1267 Sanctions Committee consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224. The GOT closely regulates charities and other nongovernmental organizations.

In August 2004, the UN Office of Drug and Crimes (UNODC) and the GOT organized a workshop to review the Togolese penal code. UNODC recommended that Togo either amend the penal code or pass separate laws on terrorism to comply with UN terrorism resolutions.

The Central Bank of West African States (BCEAO), based in Dakar, is the Central Bank for the countries in the West African Economic and Monetary Union (WAEMU): Benin, Burkina Faso, Guinea-Bissau, Cote d'Ivoire, Mali, Niger, Senegal, and Togo, all of which use the French-backed CFA franc currency. All bank deposits over approximately \$7,700 made in BCEAO member countries must be reported to the BCEAO, along with customer identification information. In September 2002, the WAEMU Council of Ministers, which oversees the BCEAO, issued a directive requesting that each member country set up a national committee under their Minister of Finance to deal with financial information as it relates to money laundering. The BCEAO is to be in charge of coordinating such committees. Each member country is now responsible for putting legislation into place to implement this directive, and the legislation is expected to be harmonized regionally.

The WAEMU Council of Ministers issued another directive in September 2002 requesting member countries to pass legislation requiring banks to freeze the accounts of any person or organization on the UN 1267 Sanctions Committee's consolidated list.

In 2000, the Economic Community of West African States (ECOWAS) established the Intergovernmental Action Group against Money Laundering (GIABA), based in Dakar, Senegal. In November 2002, GIABA hosted an anti-money laundering seminar for representatives of 14 ECOWAS members, including Togo. In July 2002, Togo participated in the 2002 West African Joint Operation Conference (WAJO) that promotes regional law enforcement cooperation against narcotics-trafficking, terrorism, and money laundering.

Togo is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. On November 27, 2003 Togo signed, but has not yet ratified, the UN Convention against Transnational Organized Crime.

The Government of Togo should criminalize money laundering for all serious crimes, criminalize terrorist financing, and enforce existing laws and regulations.

## **Tonga**

Tonga is an archipelago, located in the South Pacific, about two-thirds of the way from Hawaii to New Zealand. Tourism is the second largest source of hard currency earnings following remittances. Tonga is neither a financial center nor an offshore jurisdiction. An additional source of revenue is the registry of approximately 65 ships from 25 countries, including the United States. Tonga became a party to the UN International Convention for the Suppression of the Financing of Terrorism in December 2002.



The Reserve Bank of Tonga is the primary authority in charge of coordinating the identification of suspicious financial transactions for further investigation. Tonga has not yet established a Financial Intelligence Unit (FIU), however the Reserve Bank is responsible for conducting on site exams of Commercial banks procedures, and training staff members to spot suspicious transactions. Commercial banks are currently required to report suspicious Financial Transaction Reports (FTRs) to the Reserve Bank of Tonga. Since this requirement was instituted in 2002, there have been 5 suspicious transactions referred to the Reserve Bank for further investigation. There have been no prosecutions to date.

Tonga has proposed, but not yet enacted, new legislation to criminalize money laundering and terrorist financing. Cabinet and Parliament will consider amendments to the Money Laundering and Proceeds Act of 2000 in the middle of 2005.

Representatives from Tonga have participated in the Asia/Pacific Group on Money Laundering (APG) anti-money laundering workshops and attended seminars conducted by the Egmont Group. Tonga plans to submit an application to join the APG in 2005. Representatives from Tonga also attended several seminars in Fiji that were related to combating money laundering.

In a 2003 report to the UN Counter-Terrorism Committee, Tonga reported that its Government Committee on Money Laundering and the Financing of Terrorism was working on proposed new legislation and amendments to bring its legislative framework into line with international best practices. Tonga failed to act on that legislation in 2004.

The Government of Tonga should quickly enact legislation that specifically criminalizes money laundering and the financing of terrorism and establishes a Financial Intelligence Unit (FIU). It should follow through with its plan to join the Asia/Pacific Group on Money Laundering. It should also sign and ratify the UN Convention against Transnational Organized Crime.

## **Trinidad and Tobago**

Trinidad and Tobago has a well-developed and modern banking sector that makes it an increasingly significant regional financial center. Trinidad and Tobago (T&T) is not an offshore financial center. Illegal drug-trafficking proceeds are not known to be an important source of laundered funds in T&T, although they are implicated in some money laundering. Criminal proceeds laundered in T&T are derived primarily from domestic criminal activity and from the activity of nationals involved in crime abroad. While there is no significant black market for smuggled goods in T&T, drug money continues to support the importation of illegal arms into the country.

Financial crimes in general are increasing, particularly those involving the use of fraudulent checks and related instruments in the banking sector. Trinidad and Tobago's financial institutions are not known to engage in current transactions involving international illegal drug-trafficking proceeds that significantly affect the United States.

The Proceeds of Crime Act of 2000 (POCA) expands money laundering predicate offenses to include all serious crimes. The POCA requires financial institutions to proactively report suspicious transactions, and banks and financial institutions are required to maintain records necessary to reconstruct transactions for a number of years. Secrecy laws are limited to standard client confidentiality provisions. Failure to comply with POCA's record keeping and reporting requirements can result in a fine of TT 250,000 (approximately \$40,000) and imprisonment for two years for summary conviction, and a fine of TT 3,000,000 (approximately \$500,000) and seven years imprisonment for conviction on indictment. Upon summary conviction for money laundering, an offender can be liable for a fine of TT 25,000,000 (approximately \$4,000,000) and 25 years imprisonment. Under the POCA, any officer who aids and abets the money laundering activities of an institution can be convicted of money laundering. In addition, the POCA protects individuals who cooperate in money laundering law enforcement investigations. The POCA also enables the courts to seize the proceeds of all serious crimes, although only one property has been seized under the Act.

The Central Bank has set anti-money laundering guidelines, including due diligence provisions that apply to all financial institutions subject to the 1993 Financial Institutions Act. These include banks, finance companies, leasing corporations, merchant banks, mortgage institutions, unit trusts, credit card businesses, financial services businesses and financial intermediaries. In 2004, the Central Bank updated these guidelines, setting new minimum standards for compliance with existing regulations and informing stakeholders on proposed legislation. The Central Bank will bring large credit unions under its supervision by 2005. Also in 2004, the Government of Trinidad and Tobago (GOTT) established a fledgling Tax Fraud Investigations unit in its Inland Revenue Division to address tax evasion and non/underreported income that may have its source from money laundering activities.

GOTT customs regulations require that any sum above approximately \$3,000 (in currency or monetary instruments) entering or leaving the country be declared. GOTT Customs may restrain cash above approximately \$10,000 for 96 hours, or longer with judicial approval, pending the determination of their legitimate source. The Financial Investigations Unit (FIU) maintains a database of these transactions and analyzes them for evidence of money laundering.

There are six free trade zones in T&T where exporting of services and manufactured products, and re-exportation of manufactured products take place. There is no evidence that these zones are involved in money laundering schemes, and companies operating in these zones are required to submit quarterly tax returns and yearly audited financial statements. These companies must present their bona fides and are subject to background checks prior to being allowed to operate in these zones.

The GOTT has legislation in place that allows it to trace, freeze, and seize assets, including bank accounts. Authorities may also seize legitimate businesses if they are used to launder drug money. However, the GOTT can only restrain assets through due process at the level of the High Court—it cannot freeze assets "without undue delay," and the law only allows for criminal forfeiture of assets, not civil forfeiture.

Since January 1, 2003, the GOTT has conducted 189 financial investigations, and has issued seven production orders and eight foreign intelligence requests. To date, traffickers, organized crime organizations and terrorist organizations have not taken any retaliatory actions related to money laundering/terrorist financing investigations. In 2004, the GOTT charged one person with laundering the proceeds of fraud and seized TT 131,618 (approximately \$22,000) in related assets. In previous years, the GOTT seized a total of TT 6 million (\$1 million) and restrained TT 1 million (approximately \$167,000).

Some legal loopholes exist that allow traffickers and supporters/financiers of terrorists or terrorist organizations to shield their assets. These include the absence of financial obligations regulations and FIU legislation, the ability of attorneys to operate accounts in their client's names, the absence of suspicious transaction reporting (STR) requirements for attorneys and accountants, and legal rules that prevent courts from confiscating assets received after a defendant's sentencing.

Opposition party intransigence has stalled legislation specifically aimed at criminalizing terrorism financing, but Parliament will debate this bill again in 2005. The GOTT is developing regulations for financial sector supervision that acknowledge and monitor alternative remittance systems. The banking system has also reported the suspicious use of charitable or nonprofit entities. The GOTT has circulated the UN 1267 Sanctions Committee's consolidated lists to its financial institutions. The GOTT has also circulated the United States' list of Specially Designated Global Terrorists and other relevant EU lists. There has not yet been any identified evidence of terrorist financing in T&T.

In 1999, a MLAT with the United States entered into force, and in 2000, the United States and GOTT signed a joint statement on law enforcement cooperation, which pledges in part to expand cooperation on the detection and prosecution of money laundering and related criminal activities. While there is no mechanism in place with the United States Government (USG) for the exchange of crime and terrorism-related information, the GOTT has cooperated regularly with the USG and other governments' law enforcement agencies on issues involving drug-trafficking, terrorism, terrorist financing and other criminal investigations. The GOTT does not have legislation that specifically authorizes the sharing of forfeited assets with other countries, but has done so in the past on a case-by-case basis through bilateral agreements.

Trinidad and Tobago is a party to the 1988 UN Drug Convention and the 1992 Kingston Declaration on Money Laundering. It has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. It has not yet signed the UN International Convention for the Suppression of the Financing of Terrorism. T&T is a member of the Caribbean Financial Action Task Force (CFATF), which is headquartered in Port of Spain. It underwent a second round CFATF mutual evaluation in 2002, and will undergo a third round evaluation in April 2005. Trinidad and Tobago is also a member of the OAS Inter-American Drug Abuse Control Commission Experts Group to Control Money Laundering (OAS/CICAD).

The Government of Trinidad and Tobago should continue to work toward full implementation of its anti-money laundering laws and the improvement of its anti-money laundering/counterterrorist financing regime. Trinidad and Tobago should enact suspicious transaction reporting requirements and expand coverage of the laws to include intermediaries, such as attorneys and accountants, and exchange houses. Trinidad and Tobago also should become a party to the UN International Convention for the Suppression of the Financing of Terrorism and criminalize terrorist financing.

## **Tunisia**

Tunisia is not considered an important regional financial center due in large part to the very strict control exercised by the Central Bank over all aspects of financial transactions and the general non-convertibility of the Tunisian dinar. There is an offshore financial sector. There is no discernible money laundering activity reported to be occurring in Tunisia through formal financial institutions.

In December 2003, the Tunisian Parliament passed Law No. 2003-75, a comprehensive counterterrorism and anti-money laundering law, to support international counterterrorism efforts and to establish more severe sentences for individuals convicted of terrorist acts. This law makes it a crime to provide financial assistance or any other type of support to terrorist activities, and provides for the freezing of assets. Those suspected of violating the law can be exempted from charges, however, if they report a planned terrorist action to authorities.

Money laundering is punishable where false information is proffered relating to the illicit origin of property or income arising directly or indirectly from an offense. Money laundering also includes investing, depositing, transferring or safekeeping of property or income resulting from an offense. The law imposes obligations on financial institutions relating to identity checks, verification of transactions of suspect persons, record keeping and the declaration of transactions above certain monetary limits. The Ministry of Finance oversees operations to combat money laundering and terrorist financing.

Tunisia's 1992 Law (No. 92-52) against narcotics-trafficking also includes provisions that contribute to the combating of money laundering. Under Articles 2 and 30, anyone aiding in narcotic operations or transfers of proceeds in connection with these operations, including financial institutions, can be punished.

The Tunisian penal code also allows for the sequestering, confiscating, or seizure of assets and property in certain situations, including narcotics-trafficking and terrorist activities. The definition of "assets" is quite broad and could cover any number of financial or physical assets. Financial assets are traced by the Central Bank and the Economic Enforcement Agency, each of which has broad powers for investigating and seizing financial assets. Tunisia has no legal provisions for sharing seized criminal assets with other governments.

Financial institutions are required to gather full identifying information for personal and business accounts. In addition, all supporting documentation must be maintained for 10 years. Only certain categories of individuals and businesses are allowed to open foreign currency or convertible dinar accounts and all of these accounts are monitored by the Central Bank. Because there is no law against money laundering in general, there is no obligation for a financial institution to report suspicious activities or provisions for holding bankers responsible if their institution is used for money laundering. However, the prevailing practice is for institutions to verbally report any unusual activity to the Central Bank, which will notify the investigative Economic Enforcement Agency. There are no "secret" or numbered accounts allowed in Tunisia.

Offshore financial institutions are held to the same regulatory standards as onshore institutions. Offshore institutions undergo the same due diligence process as onshore banks and are licensed only after the Central Bank investigates their references and the Ministry of Finance approves their application. Tunisian law also makes provisions for "moral integrity" checks of major shareholders, directors, and officers of financial institutions at any time doubts may arise. Anonymous directors are not allowed. Tunisia currently has 8 offshore banks. There is foreign participation in over 2,600 Tunisian companies (2003 figures). There are several casinos in Tunisia, but Tunisians are not permitted to use them. The export of Tunisian dinars, by either residents or nonresidents, is strictly prohibited. Bearer financial instruments or shares are prohibited (Act No. 35 of 2000).

Although the Tunisian government maintains that there are no alternative fund transfer systems, since all fund transfers must go through the banks or National Post Office, it is precisely due to these restrictions and currency exchange controls that there are underground methods of moving money or transferring value in and out of the country. While a significant black market in consumer goods does exist in the country, there is no evidence that this trade is funded by illicit proceeds. Residents are generally prohibited from holding or exporting foreign currency except in certain cases (travel or business needs, etc.) Nonresidents entering Tunisia with foreign currency or other instruments are required to declare the total amount if they wish to re-export a portion (not exceeding 1,000 dinar or approximately \$840) or deposit any of the money in a Tunisian bank. Nonresidents do not need to declare currency exports under 1,000 dinar. Customs may at any time require declarations for gold or securities.

Tunisia is a founding member of the Middle East North Africa Financial Action Task Force (MENAFATF) based in Bahrain and approved in November 2004 by the governments of Algeria, Bahrain, Egypt, Jordan, Kuwait, Lebanon, Morocco, Oman, Qatar, Saudi Arabia, Syria, Tunisia, United Arab Emirates, and Yemen. The MENAFATF is a FATF-style regional body that will address money laundering and terrorist financing related issues and work to raise compliance standards throughout the region to meet international standards.

Tunisia is a party to both the 1988 UN Drug Convention and the 1999 UN International Convention for the Suppression of Financing of Terrorism. It has signed and ratified the UN Convention against Transnational Organized Crime. The Central Bank has circulated the UN 1267 Sanctions Committee's consolidated list to all of its financial institutions. To date no terrorist assets have been identified in Tunisia. Tunisia has varying bilateral agreements on "criminal matters" with 29 countries and is party to 12 international agreements on counterterrorism.

The Government of Tunisia should continue its efforts to implement its comprehensive 2003 legislation. It should establish a Financial Intelligence Unit (FIU) and require financial institutions to report suspicious transactions to that unit.

## **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. Turkey is not an offshore financial center. 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.

A substantial percentage of money laundering that takes place in Turkey appears to involve tax evasion, and informed observers estimate that as much as 50 percent of the economy is unregistered. Since tax evasion is such a large problem, the Government of Turkey (GOT) is in the process of reforming its tax administration, with the goal of improving tax collection. There is no significant black market for smuggled goods in Turkey. There are 21 free trade zones operating in Turkey, but there is no evidence that they are being used in trade-based money laundering schemes or terrorist financing operations. The GOT closely controls access to the free trade zones.

Money laundering takes place in both banks and non-bank financial institutions. Money laundering methods in Turkey include: the cross-border smuggling of currency; bank transfers into and out of the country; and the purchase of high value items such as real estate, gold, and luxury automobiles. It is

believed that Turkish-based traffickers transfer money to pay narcotics suppliers in Pakistan and Afghanistan, primarily through Istanbul exchange houses. The exchange houses then wire transfer the funds through Turkish banks to accounts in Dubai and other locations in the United Arab Emirates. The money is then paid, often through alternative remittance systems, to the Pakistani and Afghan traffickers.

Turkey criminalized money laundering in 1996 for a wide range of predicate offenses, including narcotics-related crimes, smuggling of arms and antiquities, terrorism, counterfeiting, and trafficking in human organs and in women. Whoever commits a money laundering offense shall be sentenced to imprisonment from two to five years 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 records for five years. These regulations apply to banks and a wide range of non-bank financial institutions, including insurance firms and jewelry dealers.

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 will take effect in April 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, which will also come into effect in April 2005, will facilitate asset forfeiture.

In July 2001, the Ministry of Finance issued a banking regulation circular requiring all banks, including the Central Bank, securities companies, and post office banks, 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. Additionally, non-interest-utilizing entities such as Islamic financial institutions are required to record tax identity information for all transactions. The Ministry of Finance also issued a circular mandating that a tax identity number be used in all financial transactions as of September 1, 2001. The circular applies to all Turkish banks and to branches of foreign banks operating in Turkey, as well as to other financial entities. The new requirements are intended to increase the Government's ability to track suspicious financial transactions. Turkey does not have 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. Natural persons and corporate bodies from whom information and documents are requested may not refrain from submitting the requested items by claiming the protection provided by privacy provisions in special laws, provided that the provisions related to the right of defense are reserved.

Generally speaking, Turkey does not have foreign exchange restrictions. However, Turkey does have cross-border currency reporting requirements. Except for payments for imports, invisible transactions and capital exports, banks and special finance institutions must inform authorities, within 30 days, about transfers abroad exceeding \$50,000 or its equivalent in foreign currency notes (including transfers from foreign exchange deposits). Travelers may take up to \$5,000 or its equivalent in foreign currency notes out of the country.

Since the financial crisis of 2000, the GOT has significantly tightened oversight of the banking system through an independent regulatory authority, the Banking Regulatory and Supervisory Agency (BRSA). BRSA conducts anti-money laundering compliance reviews at banks under authority delegated from MASAK. BRSA's reputation was hurt by its failure to detect a major bank fraud in 2003, but it is working to improve its capabilities in this area.

The 1996 anti-money laundering law establishes MASAK, which is part of the Ministry of Finance. MASAK, which became operational in 1997, serves as Turkey's Financial Intelligence Unit (FIU), receiving, analyzing, and referring STRs for investigation. MASAK has a pivotal role between the financial community, on the one hand, and Turkish law enforcement, investigators, and judiciary, on the other. MASAK itself is not yet functioning at the optimal level of efficiency, and is trying to strengthen its role. It would benefit from additional legal authority, continuity of senior management, training, and computers. Training and equipment needs are being addressed by a European Union

accession project, which is expected to end in June 2006. Under current law, MASAK has three functions: regulatory, financial intelligence, and investigative. Under long-pending draft legislation currently under review by relevant GOT agencies, MASAK would cede its investigative function to the public prosecutors, while retaining its regulatory and financial intelligence roles. Passage of the law is expected in early 2005.

The number of STRs being filed is quite low, even taking into consideration the fact that the Turkish economy is cash-based. A possible reason for this is the lack of safe harbor protection for bankers and other filers of STRs. Turkish officials indicated in December 2004 that the GOT has drafted legislation that will provide such protection, but it has not yet been enacted. Another reason is that many bankers do not believe that money laundering occurs through Turkish banks.

Turkey's anti-money laundering regime does not have a strong reputation for enforcement. Since its inception, MASAK has pursued more than 500 money laundering cases, but, as of December 2004, only one had resulted in a conviction-which was later overturned. Factors contributing to this low conviction rate include the fact that Turkey's police, prosecutors, judges, and investigators still need substantial training in dealing with financial crimes, a lack of coordination among law enforcement agencies and a lack of coordination between the courts that prosecute the predicate offenses and the courts that prosecute money laundering cases. Most of the cases involve non-narcotics criminal actions or tax evasion; roughly 30 percent are narcotics related. There were no arrests or prosecutions for money laundering in Turkey in 2004.

Turkey has traditionally taken a strong stance against terrorism, but the GOT still has not explicitly criminalized terrorist financing. The GOT believes that the new draft anti-money laundering law described above and the pending Law to Combat Terrorism should ameliorate the situation, in part by the inclusion of a definition of terrorist financing. In the interim, there are various laws with provisions that can be used to punish the financing of terrorism. In particular, Article 169 of the Turkish Penal Code prohibits assistance in any form to a criminal organization or to any organization which 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 and cowering people is illegal under the provisions of the Law No. 4422 on the Prevention of Benefit-Oriented Criminal Organizations. In February 2002, MASAK issued General Communiqué No. 3, which details a new type of STR to be filed by financial institutions in cases of terrorist financing. The GOT distributes to interested GOT agencies (but not financial institutions) the UNSCR 1267 Sanctions Committee's consolidated list. Financial institutions receive the consolidated list through the Turkish Bankers Association.

Another area of vulnerability in the area of terrorist financing is the GOT's loose supervision of non-profit organizations. The General Director of Foundations (GDF) issues licenses for charities and oversees them. The GDF requires charities to verify and prove their funding sources and to have bylaws. Charities are audited by the GDF and are subject to being shut down if they act outside the bylaws. However, the GOT does not have other oversight mechanisms, such as requiring the publication of annual reports or periodic reporting to competent authorities. In addition, there is no central registry of charities. The GOT has taken no steps to regulate or register alternative remittance systems.

The GOT has the authority to identify and freeze only the assets of individuals and entities on the UNSCR 1267 Sanctions Committee's consolidated list. The Council of Ministers promulgated a decree (2001/2483) on December 22, 2001 to freeze all the funds and financial assets of individuals and organizations included on the UN list. If enacted, the Law on the Fight Against Terrorism would authorize the dissolution of associations, foundations, and unions that are found to have lent support to terror movements. Additionally, their assets would be subject to confiscation. 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 consolidated list. In the past year, the assets of 241 individuals and organizations have been frozen under the Council of Minister's Decrees on the grounds of being connected to terrorist organizations or terrorist activities. One individual and two organizations were found to have assets in Turkey. All of the funds and assets of these parties have been frozen by relevant GOT authorities.

Turkey also has in place a system for identifying, tracing, freezing, and seizing assets that are not related to terrorism, although Turkish law allows for only criminal forfeiture not for the administrative freezing of assets. The anti-money laundering law, Article 7, 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, Article 36 of the Criminal Code provides 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, support terrorist activity, or are otherwise related to other criminal proceeds. Property or its value that is confiscated is transferred to the Treasury.

The government enforces existing drug-related asset seizure 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 non-bank 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. The GOT is expected to participate in a meeting in Vienna in January 2005 to prepare a UN model bilateral agreement on the disposal of confiscated proceeds of crime.

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. However, problems remain in terms of timely information sharing by Turkey with other countries, law enforcement and counterterrorist financing agencies.

Turkey is a member of the Financial Action Task Force (FATF). The 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, and it will come into force on February 1, 2005. Turkey has signed, but not yet ratified, the UN Convention against Corruption. However, implementation efforts on UN anti-financial crime conventions are weak, and Turkey is not believed to be in conformity with the FATF's Special Recommendations on Terrorist Financing. The GOT asserts that legislation being prepared in early 2005 will bring Turkey into conformity with all international counterterrorist financing standards.

The Government of Turkey has publicly declared its commitment to fight money laundering and terrorist financing. However, it needs to strengthen its legislative basis for this by swiftly enacting the draft laws to strengthen MASAK's powers and to criminalize terrorist financing. Turkey should also provide training for its prosecutors, judges, and investigators. Turkey should improve the coordination among the various entities charged with responsibility in its anti-money laundering/counterterrorist financing regime and between the courts, in order to increase successful investigations and convictions for money laundering. Turkey should enact its safe harbor bill to protect the filers of STRs, which may result in increased filings. Turkey should also regulate and investigate alternative remittance networks to thwart misuse by terrorist organizations or their supporters. It should also strengthen its oversight of charities.

## **Turkmenistan**

Turkmenistan is not an important regional financial center; there are only four international banks and a small, underdeveloped financial sector. Foreign companies operate six hotels and casinos in Turkmenistan. These entities could be vulnerable to financial fraud and used for money laundering.

Turkmenistan's national currency, the Turkmen Manat, has an unofficial, but generally accepted, exchange rate that is four times the official rate, creating an environment where money laundering is possible. Turkmenistan has no offshore companies or banks.

The Turkmen Criminal Code of June 12, 1997, Article 242 (Legalization of illegally obtained funds or other property) prohibits money laundering.

Turkmenistan's Law on currency regulations of October 8, 1993, defines general principles for conducting currency operations within the domestic and international accounts of Turkmenistan. It also details authorities and functions of state agencies in currency regulations and management of currency resources, rights and responsibilities of residents and non-residents in regard to ownership, use and handling of hard currency, directions of currency control, and responsibility for violating currency legislation. According to Presidential Decree No. 4715 of June 15, 2000, "Measures to Strengthen Currency Regulations in Turkmenistan," Turkmen ministries, departments, state enterprises and organizations are prohibited from opening bank accounts abroad except as specifically permitted by Turkmen legislation.

Presidential Resolution No. 0210/02-2 of October 17, 1995, gives the Central Bank of Turkmenistan (CBT) authority over all international financial transactions. Under this resolution, any entity making an electronic transfer of funds to an account abroad must provide documentation establishing the source of the money. The CBT regulations also permit an individual to transfer funds abroad of no more than \$15,000 every three months. Presidential Decree No. 5976 of November 20, 2002, "Strengthening the Regulations of Turkmen Bank Operations carried out in Foreign Currency," orders Turkmenistan banks to carry out correspondent, deposit, investment and other operations in foreign currency outside Turkmenistan only through open correspondent accounts in the CBT or State Foreign Economic Relations Bank ("Vnesheconombank").

Turkmenistan's tax inspectorate is responsible for uncovering any irregularities. If any irregularities are discovered, the tax inspectorate turns the matter over to Turkmen law enforcement for investigation. To date, no cases have been reported.

The current Law on Free Economic Zones in Turkmenistan adopted in 1993, and amended in 1994, determines the legal regime for conducting business in these zones, guarantees the rights of both foreign and domestic investors, forbids nationalization of enterprises and discrimination against foreign investors, and provides guarantees to foreign investors for exporting production and repatriating after-tax profits. All related enterprises are exempt from taxes on profits for the first three years of profitable operation. All goods and properties must be declared when imported into or exported from free economic zones. There are ten free economic zones in Turkmenistan including: Mary-Bayramali, Okarem-Hazar (Cheleken), Turkmenabat-Seyidi, Baharly-Serdar, Dashoguz Airport, Ashgabat-Anau, Ashgabat-Abadan, Ashgabat International Airport, Serakhs, and Guneshli Turkmenistan near Anau. The first seven zones were created in 1992, and the Serakhs zone was established in 1996. Two more zones, the international airport zone in Ashgabat and the Guneshli Turkmenistan zone near Anau, were created in 1997.

Presidential Decree No. 6097 of January 24, 2003, authorizes the Turkmenistan Supreme Court to open a centralized deposit account at the CBT for receiving payments from illegal enrichment, compensation of material loss or other assets obtained illegally and seized during inspection, investigation, and court trials for all crimes, including: organized crime, drug-trafficking and terrorist financing. The assets will remain in the Supreme Court account until the announcement of the court's final verdict on the case or until another decision is made.

The Turkmenistan Antiterrorism Law of August 15, 2003, authorizes the government to freeze resources and/or other financial assets, deposits, economic resources, and material values of: individuals who commit or attempt to commit terrorist acts, or contribute to their commitment; organizations directly or indirectly placed under ownership or under control of such individuals; and, individuals and organizations acting on behalf of the above individuals and organizations, including any assets acquired or received through the use of property directly or indirectly belonging to or controlled by such individuals and/or organizations. Turkmen counterterrorism laws require Turkmenistan to cooperate with foreign states and international organizations in terrorism matters and



render assistance to other states in criminal investigations and prosecutions of individuals involved in financing or supporting terrorist activities.

The Ministry of Foreign Affairs reports that it distributes information regarding designated individuals and organizations subject to asset forfeiture, provided by the United States, to the Ministry of Finance, the Ministry of National Security, the Ministry of Internal Affairs, and other concerned agencies.

Turkmenistan is a party to the 1988 UN Drug Convention.

The Government of Turkmenistan should enact appropriate legislation and take steps to implement a comprehensive anti-money laundering regime capable of thwarting terrorist financing that conforms to international standards. Turkmenistan should sign and ratify the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. Turkmenistan should also consider joining or becoming an observer to the new Eurasian Group on Combating Money Laundering and Financing of Terrorism, a Financial Action Task Force (FATF) Style Regional Body established in October 2004.

### **Turks and Caicos**

The Turks and Caicos Islands (TCI) is a Caribbean overseas territory of the United Kingdom (UK). 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. 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 a large offshore financial services sector as well as because of bank and corporate secrecy laws and Internet gaming activities. There is no updated information to add for 2004.

As of 2003, the TCI's offshore sector has eight banks (five of which also deal with onshore clientele), approximately 2,500 insurance companies, 1,000 trusts, and 13,000 "exempt companies" that are IBCs, including those formed by the Enron Corporation. 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. The Financial Services Commission employs a staff of 14 and conducts limited on-site inspections. The FSC became a statutory body under the Financial Services Commission Ordinance 2001 and became operational in March 2002, and now reports directly to the Governor.

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 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.

The 1998 Proceeds of Crime Ordinance criminalizes money laundering related to all crimes and establishes extensive asset forfeiture provisions and "safe harbor" protection for good faith compliance with reporting requirements. The Law 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 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 five 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 banking,

insurance, trustees, and mutual funds. 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 non-statutory 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 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, but the Ordinance has not yet been enacted. No legislation has yet 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.

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 have put in place a comprehensive system to combat money laundering with the relevant legislative framework and an established FIU. The FSC has made steady progress in developing its regulatory capability and has some experienced senior staff. However, the current regulatory structure is not fully in accordance with international standards. The Turks and Caicos Islands should criminalize the financing of terrorists and terrorism, and enhance its on-site supervision program. Turks and Caicos Islands should expand efforts to cooperate with foreign law enforcement and administrative authorities. Turks and Caicos Islands should 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 Island's financial sector.

## **Uganda**

Uganda is not a regional financial center and is not a major hub for narcotics trafficking or terror finance. Some money laundering occurs in Uganda. It appears that a large percentage of the money laundering occurring in Uganda stems from domestic criminal actions, often related to smuggling counterfeit products, and other financial fraud. Reportedly, large drug-trafficking organizations, organized crime groups, and terror groups have historically not played a leading role in money laundering activities in the country. However, there have been reports during the past year that certain significant figures may be involved in organized international money laundering schemes, possibly related to narcotics trafficking. The Government of Uganda (GOU) does not monitor cross-border financial activities. The GOU has finally begun to draft legislation to confront money laundering on a broad scale.

Money laundering also occurs in the informal financial sectors. Many Ugandans working abroad use alternate, cash-based, informal remittance systems to send money back to their families. Many establishments in Kampala accept U.S. dollars for cash transactions. Under legislation passed in 2004, foreign exchange bureaus are not authorized to transfer money abroad. The GOU has no effective means to prevent money launderers from accessing the many charitable and faith-based organizations that operate in Uganda. Moreover, to date, the GOU has not been able to document the level to which money launderers have used these entities.

Uganda does not have an offshore banking sector. The Special Economic Zones Bill of 2002 authorized the creation of export-processing zones (EPZs) and free trade areas within Uganda, and the GOU recently received a World Bank credit to establish EPZs. However, the GOU has not yet developed either EPZs or free trade areas. In 2001, Uganda criminalized narcotics-related money laundering. In 2003, the Bank of Uganda issued know your customer guidelines for Ugandan commercial banks, though it currently is unwilling to enforce compliance. In December 2003, the Ministry of Finance submitted to Parliament a comprehensive anti-money laundering bill based on the Financial Action Task Force's (FATF's) Forty Recommendations on Money Laundering. This legislation would criminalize money laundering for all serious crimes. However, the legislation did not pass during the past year. Until the draft AML legislation passes, the GOU maintains only limited authority and ability to investigate and prosecute money laundering related violations. To date, the GOU has not prosecuted anyone for narcotics-related or any other crime-related money laundering.

Beginning in 2004, the Bank of Uganda has circulated to financial institutions the list of individuals and entities included on the UNSCR 1267 Sanctions Committee's consolidated list. The Uganda Anti-Terrorism Act (ATA) of 2002, which entered into effect in June 2002, criminalized contributing, soliciting, controlling, or managing funds used to support terrorism or terror organizations. Despite the ATA, GOU authorities believe they have limited powers to freeze or seize terrorist finance-related assets. The draft AML would significantly expand this authority allow the GOU to seize all proceeds of crime.

Uganda is a member of the East and Southern African Anti-Money Laundering Group (ESAAMLG) and served as chair from August 2003 to August 2004. Uganda is a party to the 1988 UN Drug Convention and the UN International Convention for the Suppression of the Financing of Terrorism. It has signed, but not yet ratified, the United Nations Convention against Transnational Organized Crime. At this time, Uganda and the United States do not have formal agreements to facilitate the exchange of information and records in connection with investigations relating to narcotics, terrorism, and other crimes. Nevertheless, Ugandan authorities have cooperated with U.S. law enforcement efforts. In May 2004, at the request of the United States, the GOU detained and deported two U.S. citizens to face money laundering and wire fraud charges in the U.S.

The Government of Uganda should act on the draft legislation pending since December 2003 and enact comprehensive anti-money laundering legislation that meets international standards and construct a viable anti-money laundering regime capable of thwarting terrorist financing. It should ratify the UN Convention against Transnational Organized Crime.

## **Ukraine**

Ukraine has made rapid progress over the past two years in adopting, enacting and implementing comprehensive anti-money laundering legislation. However, high-level and widespread corruption, organized crime, smuggling, tax evasion, and other economic crimes continue to plague Ukraine's economy. Money laundering in Ukraine is not primarily related to proceeds from narcotics-trafficking, although this activity does generate at least a portion of organized crime income. Illicit proceeds also originate in criminal activities such as fraud, manipulation of the privatization process, fictitious entrepreneurship, smuggling of goods, trafficking in weapons and human beings, and large-scale corruption by government officials and others. Retail outlets that sell luxury goods and other businesses (including casinos and some restaurants) in Kiev and elsewhere are suspected of being fronts for money laundering and/or tax evasion. In June 2004, a federal jury in the United States convicted Ukraine's former Prime Minister, Pavlo Lazarenko, of money laundering, conspiracy to launder money, wire fraud, and transportation of stolen property. Ukraine provided assistance to the United States in connection with this prosecution.

According to Ministry of the Interior reports, banking fraud was the most common economic crime for the period of January through September 2004. The Ministry of Interior registered 39,300 economic crimes, or 6.2 percent more than over the same period of 2003, including 371 cases of money laundering, 3,500 cases of bank fraud, and 1,700 cases of smuggling. The market for smuggled goods remains significant in Ukraine, especially for textiles, automobiles, alcohol, and tobacco products.

Ukraine has created eleven Free Economic Zones (FEZs), and nine Priority Development Territories (PDTs), reportedly covering some 10 percent of Ukrainian territory. In August 2002, the Cabinet of Ministers introduced a moratorium on the establishment of FEZs and PDTs until January 1, 2005. There is a separate law for each FEZ that defines a set of tax exemptions enjoyed by the FEZ. Creation of FEZs was originally intended to enliven business and attract investment to depressed territories, but effectiveness of their operation is disputable. Legislative loopholes permit companies to misuse FEZ status, and to avoid taxes and import duties. The State Department of Financial Monitoring has uniform policy regarding economic entities operating throughout the country and does not envisage any specific provisions on FEZs.

When the Financial Action Task Force (FATF), in September 2001, placed Ukraine on the list of non-cooperative countries and territories in the fight against money laundering (NCCT), 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. At its September 2002 plenary, FATF extended its original October 2002 deadline, by which Ukraine had to enact comprehensive, effective anti-money laundering legislation, or it would face the possibility of a recommendation for countermeasures from the FATF member countries, until December 15, 2002. On November 28, 2002, President Kuchma signed into law Ukrainian Law No. 249-IV, an anti-money laundering package "On Prevention and Counteraction of the Legalization (Laundering) of the Proceeds from Crime" (the Basic AML Law). On December 20, 2002, the FATF determined that Ukraine's new AML statute did not meet international standards and announced a recommendation that FATF members impose countermeasures on Ukraine. Under Section 311 of the USA PATRIOT Act, on December 20, 2002, the United States designated Ukraine as a jurisdiction of primary money laundering concern. In response to the imminent threat of countermeasures, Ukraine passed further comprehensive legislative amendments in December 2002 and February 2003, in accordance with FATF recommendations. 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.

By passing comprehensive anti-money laundering legislation, Ukraine was not only able to avoid the countermeasures threatened by the FATF, but to initiate the process of NCCT de-listing. At the FATF plenary in September 2003, Ukraine was invited to submit an implementation plan, and upon review by the FATF Europe Review Group (ERG), 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 ERG, and Ukraine was accordingly de-listed at the FATF plenary on February 25, 2004. As a condition for de-listing, Ukraine continues to undergo monitoring by the FATF on implementation of its AML regime.

As a member of the Council of Europe, Ukraine has undergone two mutual evaluations by that group's Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), in May 2000 and September 2003. Although Ukraine criminalized drug money laundering in 1995, the initial 2000 mutual evaluation report was highly critical of Ukraine. The 2003 evaluation presented quite a different finding, as evaluators noted that a number of the previously noted deficiencies had been remedied, especially with regard to passage of the basic AML law in November 2002.

Two subsequent sets of amendments to the Basic AML Law, adopted in December 2002 and February 2003, have further helped bring Ukraine into compliance with internationally-recognized standards, as set forth by the FATF, UN and European Union (EU) conventions and directives on money laundering, and the Basel Committee's "Core Principles for Effective Banking Supervision".

Effective September 1, 2001, the Government of Ukraine (GOU) criminalized non-drug money laundering in the Criminal Code of Ukraine. Subsequent amendments adopted in January 2003 include willful blindness provisions and expand the scope of predicate crimes for money laundering to include, with certain exceptions, any action that is punishable under the criminal code by imprisonment of three years. Provisions in the criminal code also address drug-related money laundering offenses and provide for the confiscation of proceeds generated by criminal activities.

The GOU enacted the "Act on Banks and Banking Activities"(Act) of January 2001, which imposes anti-money laundering measures 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. Further amendments in February 2003 require banks to conduct due diligence to identify beneficial account owners prior to opening an account or conducting certain transactions, and to maintain records on suspicious transactions and the people carrying them out for a period of five years. The AML legislation also mandates the establishment of AML procedures in first-line financial institutions such as banks; stock, securities, and commodity brokers; and insurance companies, among other entities. Subsequent amendments mandate establishment of bank compliance programs and the appointment of bank compliance officers who may be subject to criminal liability for non-compliance. They also require employees of entities that carry out financial transactions to report transactions suspected for money laundering or terrorism finance. The AML legislation includes a "safe harbor" provision that protects reporting institutions from liability for cooperating with law enforcement agencies. In June 2004, the National Bank of Ukraine (NBU) drafted amendments to the Act, strengthening anti-money laundering requirements for banks. In particular, it mandates that the AML compliance officer also be a bank director, forbids banks to have correspondent accounts with shell banks, and authorizes the NBU to obtain information from other state authorities and legal persons in order to determine the business reputation and financial circumstances of prospective bank owners and directors. Travelers must declare cross-border transportation of cash sums exceeding \$1000.

In August 2001, "The Law on Financial Services and State Regulation of the Market of Financial Services" (August 2001 Law) was signed. The August 2001 Law establishes regulatory controls over non-bank financial institutions that manage insurance, pension accounts, financial loans, or "any other financial services involving savings and money from individuals." Specifically, it imposes record keeping requirements on covered entities and identifies the responsibilities of regulatory agencies. The August 2001 Law creates the State Commission on Regulation of Financial Services Markets, which, together with the NBU and the State Commission on Securities and the Stock Exchange, has the primary responsibility for regulating financial services markets. Amendments introduced in February 2003 set forth additional requirements similar to those prescribed for banks for all non-bank financial institutions. Additionally, in August 2003, the State Commission established a State Register of financial institutions; as of December 2004, it contains information on over 1200 non-bank financial institutions.

Significantly, amendments to Article 11 of the August 2001 Law reduce the monetary threshold over which transactions and operations are subject to compulsory financial monitoring, from Ukrainian hryvnias (UAH) 300,000 (approximately \$57,750) for cashless payments and UAH 100,000 (approximately \$19,250) for payments in cash to one single amount for both, UAH 80,000 (approximately \$15,400). The compulsory transaction-reporting threshold applies only if the transaction also meets one or more suspicious activity indicators as set forth in the law. Any transaction that is suspected of being connected to terrorist activity is to be reported to the appropriate authorities immediately.

In November 2004, the GOU approved and sent to Parliament for review a draft law "On Amending Some Legislative Acts of Ukraine on Prevention to Legalization (Laundering) of the Proceeds from Crime and Terrorist Financing." The draft law, which proposes amendments to several pieces of existing legislation, is designed to bring Ukraine into compliance with the revised FATF Forty Recommendations, the Special Recommendations on Terrorist Financing, and the UN International Convention for the Suppression of the Financing of Terrorism. Proposed amendments to the Basic AML Law include expanding the list of covered entities to include financial intermediaries, such as real estate dealers, lawyers, notaries, advocates, public accountants, auditors, dealers in precious metals and stones, and others. These amendments also would widen the list of supervisory and regulatory

financial monitoring authorities over such entities; in particular, designating the Ministry of Finance as responsible for gambling institutions, legal persons that organize any lotteries, dealers in precious metals and precious stones, public accountants and auditors; the State Committee on Land Resources for real estate dealers (realtors); the Ministry of Justice for notaries, lawyers, businesses providing incorporation and registration services for enterprises as well as management services of enterprises and property; and the Ministry of Transport and Communications for postal operators.

Additional proposed amendments to the Basic AML law include provisions to allow financial intermediaries to suspend suspected money laundering or terrorist finance related financial transactions for two working days and to require them to notify the Financial Intelligence Unit (FIU)-the entity to be designated as the authority for combating terrorist financing in Ukraine-of the suspension within one day. The FIU is authorized to suspend the transaction for an additional five working days. Customer due diligence (CDD) requirements for financial intermediaries would also be expanded to bring them into conformity with the revised FATF recommendations on customer identification and establishment of beneficial ownership. The Code of Ukraine on Administrative Offenses also would be supplemented to provide new supervisory and regulatory bodies with the authority to impose administrative fines on financial intermediaries for non-compliance with AML requirements. Notably, the draft law also amends the Ukrainian Criminal Code, criminalizing terrorist financing as a separate crime, and lowering the threshold of predicate offenses for money laundering from three to two years. Although the first reading in Parliament did not secure enough votes for adoption of the draft law, it is currently under review and will most likely undergo a second vote in 2005.

On December 10, 2001, the Ukrainian Presidential Decree "On Measures to Counteract Legalization (Laundering) of Proceeds from Crimes" mandated the creation of the State Department of Financial Monitoring (FMD) by January 1, 2002, to function as Ukraine's FIU. The FMD became operational on June 12, 2003. Under the terms of this decree, the FMD is an independent authority, administratively subordinated to the Ministry of Finance, and is the sole agency authorized to receive and analyze financial information from first line financial institutions. Ukraine's basic AML law establishes a two-tiered system of financial monitoring and combating of criminal proceeds, including terrorist financing: entities of initial financial monitoring, or those legal entities that carry out financial transactions; and entities of state financial monitoring, or those regulating entities charged with regulation and supervision of the activities of the service providers. The overall regulatory authority in the system is vested in the FMD. The FMD is an administrative agency with no investigative or arrest authority. It is authorized to collect and analyze suspicious transactions, including those related to terrorist financing, and to transfer financial intelligence information to competent law enforcement authorities for investigation. By presidential decree on September 28, 2004, the FMD was elevated to a Central Executive agency with special status. The change, which takes effect on January 1, 2005, subordinates the new agency, known as the Financial Monitoring Committee (FMC), directly to the Cabinet of Ministers. Beginning January 2005, the FMD plans to open territorial offices in each of Ukraine's 27 administrative regions. Due to the change in status of the FIU and also to the creation of the territorial offices, the FIU staff size has correspondingly been increased from 100 to 338 persons.

In 2003, the FMD received 220,427 suspicious transaction reports (STRs), the bulk of which have been reported by banks. Approximately ten percent of these were identified by the FMD for "active research" and 3,211 were sent to competent law enforcement agencies as part of 18 case referrals. In 2004, the FMD received 725,959 STRs, 96.6 percent filed by banks. Of the 3.4 percent of STRs filed by non-banking financial intermediaries, the insurance sector comprised over 67 percent of the reporting. The FMD referred 164 cases comprising 20,929 STR filings to law enforcement authorities for the calendar year, seven of which were linked to terrorist financing.

From June 12, 2003, the date the FMD became operational, through December 31, 2004, FMD has referred a total of 182 cases to law enforcement agencies, 44 of which were sent to the General Prosecutor's Office (GPO), 42 to the Ministry of Interior, 50 to the Security Service of Ukraine, and 46 to the State Tax Administration of Ukraine. As a result of subsequent investigation, law enforcement agencies initiated 32 criminal cases based upon 67 original case referrals. Eleven of these cases were initiated based on suspicion of money laundering, with predicate offenses ranging from fraud, fictitious entrepreneurship, unlawful activity with payment cards, forgery, and abuse of power or official position. Three criminal cases have been passed to the courts and others are currently under investigation. Additionally, during the first eight months of 2004, the State Security Service filed 71 criminal cases on money laundering charges. The Ministry of Interior reported that over 10 months of 2004 it detected

398 crimes connected to money laundering. Eighty-three of them were committed by criminal groups involved in laundering proceeds from trafficking in drugs or arms, smuggling and tax evasion.

Ukraine is in the initial stages of drafting a law that may permit asset forfeiture. Ukraine has yet to establish a system and a legal basis for freezing and seizing assets derived from serious crimes. In response to earlier criticisms by the FATF regarding lack of coordination and information-sharing among agencies, the Cabinet of Ministers issued Decree No. 1896 on December 10, 2003, establishing a Single State Informational System (SSIS) of Prevention and Counteraction of Money Laundering and Terrorism Financing. This is a functioning system that electronically unites databases of 17 ministries and agencies through a central server located at the FIU and sub-servers at each of the participating state agencies, thereby allowing the FIU electronic access to virtually all information housed in the databases of the other agencies. In order to foster better interagency cooperation, on September 22, 2004, the Cabinet of Ministers adopted a resolution establishing a Governmental Coordination Council On Functioning of a Single State Informational System. The Council will be comprised of high-level governmental officials in the Cabinet of Ministers, Ministries of Economy, Finance and Interior, Customs Office, and other agencies, including the FIU, and will address organizational issues of SSIS functioning and expansion.

Amendments to criminalize terrorist financing and to vest the Security Service of Ukraine with authority to investigate terrorist financing have been proposed as part of the draft law submitted to Parliament in November 2004. The GOU has cooperated with U.S. Government efforts to track and freeze the financial assets of terrorists and terrorist organizations. The NBU, State Tax Administration, Ministry of Finance, and State Security Service are fully aware of U.S. Executive Order (E.O.) 13224 and subsequent updates and addenda to the lists of terrorists and terrorist organizations. All agencies have tracked data that was provided and have exchanged information. The NBU has issued orders to banks to freeze accounts of individuals or organizations listed in the E.O. Ukraine plans to sign a U.S.-Ukraine agreement on mutual admission and actions on a list of persons/entities related to terrorist activities.

The GOU has also taken steps to implement UN Security Council resolutions relevant to fighting terrorism. The Cabinet of Ministers, on December 22, 1999, issued a resolution ordering agencies and banks to freeze assets and funds of the entities and individuals on the UNSCR 1267 Sanctions Committee's consolidated list. A Cabinet of Ministers resolution instructed the NBU to order all banks to comply with UNSCR 1333. In response to these measures, the NBU sent letters to regional departments and commercial banks to execute all applicable provisions of UNSCRs 1267 and 1333. The FMD acknowledges the existence and use of alternative remittance systems such as hawala. FMD personnel have attended seminars and exchanged information about such systems. The FMD and security agencies monitor charitable organizations and other non-profit entities that might be used to finance terrorism.

Ukraine will host the development of a prototype system for enhancing international data exchange and case collaboration (INDECCS). It is expected that the prototype will be completed in the spring of 2005 for presentation and review by international AML/CTF organizations. If successful, the new system promises to dramatically enhance the speed and quality of international information exchange, and will introduce new real time collaboration capabilities among and between participating countries.

FMD also has authority to conclude interagency agreements, and can exchange intelligence on financial transactions with a money laundering or terrorist financing nexus with other FIUs. In June 2004, FMD joined the Egmont Group. As of December 2004, 19 memoranda of understanding were concluded between the FMD and the FIUs of Russia, the Slovak Republic, Estonia, Italy, Spain, Belgium, the Czech Republic, Colombia, Georgia, France, Serbia, Macedonia, Slovenia, Poland, Romania, Portugal, Cyprus, Brazil, and Panama. However, as a member of Egmont, Ukraine may also exchange information with any other FIU whose legislation similarly allows information exchange without a memorandum of understanding in place. Under this framework, the FMD regularly exchanges information with the United States and other Egmont members, and has reported a 50 percent increase in information exchange with foreign FIUs since its accession to the Egmont Group.

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. The GOU has also participated in GUUAM (Georgia, Ukraine, Uzbekistan, Azerbaijan and Moldova) for the development of a joint law enforcement center that would cover asset seizure issues on a regional basis.

Ukraine ratified the UN Convention against Transnational Organized Crime in May 2004. Ukraine is a party to the 1988 UN Drug Convention as well as the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. In March 2002, the European Convention on the Suppression of Terrorism was signed. Ukraine ratified the UN International Convention for the Suppression of the Financing of Terrorism in September 2002. Ukraine also became a signatory to the UN Convention against Corruption.

The Government of Ukraine has demonstrated considerable political will to combat money laundering by strengthening, clarifying, and implementing its newly adopted laws. As evidenced by the positive steps taken by its FIU, the NBU, and other actors in the financial and legal sectors, Ukraine has clearly shown its ability to implement a comprehensive anti-money laundering regime. Ukraine should criminalize the financing and support of terrorists and terrorism. Ukraine should adopt an asset forfeiture regime. Ukraine should continue to enhance and implement its newly adopted anti-money laundering regime, and should enact its pending legislation to expand coverage of its anti-money laundering laws to financial intermediaries. Law enforcement agencies should give higher priority to investigating money laundering cases. Both law enforcement officers and the judiciary lack a fundamental understanding of the nature of money laundering as a criminal offense. Both should be provided training in the theoretical and practical aspects of investigation and prosecution of money laundering.

### **United Arab Emirates**

The United Arab Emirates (UAE) is an important financial center for the Gulf region. The UAE is still a largely cash-based society. However, the financial sector is modern and progressive. Dubai, in particular, is a major international banking center. There is also a growing offshore sector. The UAE's robust economic development, political stability, and liberal business environment have attracted a massive influx of people and capital. Because of the UAE's geographic location and role as the primary transportation and trading hub for the Gulf States, East Africa, and South Asia, and with its expanding trade ties with the countries of the former Soviet Union, the UAE has the potential to be a major center for money laundering. The large number of resident expatriates from the above regions, many of whom are engaged in legitimate trade with their homelands, or send remittances there, exacerbates that potential. Approximately 80 percent of the UAE population is comprised of non-nationals. The laundering of proceeds from the illegal narcotics trade is known to occur in UAE, and given the country's close proximity to Afghanistan, where most of the world's opium is produced, such narcotics-trafficking is a likely source. In addition, the potential exploitation of the UAE financial system by foreign terrorist groups is a serious concern.

Following the September 11 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 and, in close concert with the United States, to freeze the funds of groups with terrorist links, including the Al-Barakat organization, which was headquartered in Dubai. Both federal and Emirate-level officials have gone on record as recognizing the threat money laundering activities in the UAE pose to the nation's security. They have taken significant steps in 2004 to better monitor cash flows through the UAE financial system and to cooperate with international efforts to combat terrorist financing, including the passage of a law that specifically criminalizes terrorist financing.

Law No. 4 of 2002 criminalizes all forms of money laundering activities. The law calls for stringent reporting requirements for wire transfers exceeding \$545 and currency importation/exportation limits set roughly at \$11,700. The law imposes stiff criminal penalties (up to seven years in prison and a fine of up to 300,000 dirhams (\$81,700), as well as seizure of assets if found guilty) for money laundering. It also provides safe harbor provisions for those who report such crimes. Banks and other financial institutions (exchange houses, investment companies, and brokerage houses) are supervised by the Central Bank (CB) and are required to follow strict "know your customer" guidelines; all financial



transactions over \$54,000, regardless of their nature, must be reported to the CB. Financial institutions also are required to maintain records on transactions for five years.

In July 2000, the UAE established the National Anti-Money Laundering Committee (NAMLC), under the Chairmanship of the Central Bank's Governor, with representatives from the Ministries of Interior, Justice, Finance, and Economy; the National Customs Board; the Secretary General of the Municipalities; the Federation of the Chambers of Commerce; and five major banks and money exchange houses (as observers). It has overall responsibility for coordinating anti-money laundering policy.

The supervision of the UAE banking and financial sector falls under the authority of the CB. The CB issues instructions and recommendations as it deems appropriate and is permitted to take any necessary measure to ensure the integrity of the UAE's financial system. The CB issues licenses to financial institutions under its supervision and may impose administrative sanctions for compliance violations. The CB has issued a number of circulars requiring customer identification and providing for a basic suspicious transaction-reporting obligation. When suspicious activity is reported from a financial institution, the Central Bank is able to freeze suspect funds, make appropriate inquiries, and coordinate with law enforcement officials.

In an effort to consolidate and expand anti-money laundering requirements for the financial sector, the CB issued Circular 24/2000 in November 2000 to all banks, money exchanges, finance companies, and other financial institutions operating in the UAE. This circular 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 Circular 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.

On July 29, 2004, the UAE strengthened its legal authority to combat terrorism and terrorist financing, by passing Federal Law Number 1 of 2004 on Combating Terror Crimes (Law No. 1/2004). The law 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 "non-conventional weapons" or their components, with the intent to use them in a terrorist activity.

Law No. 1/2004 specifically criminalizes the funding of terrorist activities or terrorist organizations. 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," whether or not 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.

Law No. 1/2004 also sets up a "National Anti-Terror Committee" with representatives from the Ministries of Foreign Affairs, Interior, Justice, and Defense, the Central Bank, the State Security Department, and the Federal Customs Authority. The Committee serves as a UAE interagency liaison, implements UN Security Council Resolutions on terrorism, and shares information with its foreign counterparts as well as with the United Nations (UN).

Law 4/2002 provided for the establishment of the Anti-Money Laundering and Suspicious Case Unit (AMLSCU), which acts as the Financial Intelligence Unit (FIU) and is housed within the CB. Financial institutions under the supervision of the CB are required to report suspicious transactions to the AMLSCU, which is charged with examining them and coordinating the release of information with law enforcement and judicial authorities. It has the authority to request information from foreign regulatory authorities in carrying out its preliminary investigation of suspicious transaction reports. The

AMLSCU—a member of the Egmont Group since June 2002—exchanges information with foreign FIUs on a reciprocal basis, and has provided information relating to investigations carried out by the United States and other countries. In June 2004, the AMLSCU hosted a joint training session in Abu Dhabi for the nations of South Asia that are taking steps toward setting up their anti-money laundering regimes, including FIUs. The seminar focused on building an effective anti-money laundering regime, information technology issues, bilateral cooperation and mutual assistance, regulatory issues, hawala, international initiatives, and basic intelligence analysis.

From December 2000 to November 30, 2004, the AMLSCU received 2259 reports of suspicious transactions; of that number, 2148 were investigated by either the AMLSCU, the Central Bank, or law enforcement officials. In 27 cases, the Central Bank issued freeze orders and referred the cases to the Public Prosecutor; 12 of those cases are currently in the process of prosecution for money laundering, and 9 are in the process of judgment for money laundering and confiscation of proceeds.

Some money laundering in the UAE occurs in the formal banking system, including the numerous money exchange houses, but it is more prevalent in the informal and largely undocumented hawala remittance system. The fact that hawala is an undocumented and nontransparent system, and is highly resilient in response to enforcement and regulatory efforts, makes it difficult to control and an attractive mechanism for terrorist and criminal exploitation. The UAE has begun to make progress in confronting its vulnerability to the unregulated use of hawala. New regulations to improve oversight of the hawala system were implemented in 2002, when the CB required hawala brokers to register, submit the names and addresses of senders and beneficiaries, and to file suspicious transaction reports. As of January 2005, the number of applicants to obtain a hawala dar (hawala brokers) certificate reached 151, of which 128 were issued and the remaining 23 are in the process of fulfilling the requirements. There is no accurate estimate of the total number of UAE-based hawala brokers.

The UAE hosted its second International Conference on Hawala in April 2004, which was attended by approximately 350 participants. Delegates included government officials, executives of supervisory institutions, banking experts, and law enforcement officials from the United States, Latin America, Asia, and Europe. The conference statement recognized the key role that hawala and other informal funds transfer systems play in facilitating remittances, particularly those of migrant workers, although such systems can be abused for illegal activities. The conference reaffirmed the "The Abu Dhabi Declaration on Hawala," which calls for the establishment of a sound mechanism to regulate hawala.

The new attention on hawala is encouraging more people in the country to use regulated exchange houses. Representatives of money exchange business noted that their sector could transfer money anywhere, even to a private residence, for a fee competitive with hawala, persuading many to use the formal, and more secure, banking network.

In January 2002, the UAE CB published a declaration requirement for cash imported into the country above \$10,900. The regulations provide customs services with the authority to seize undeclared cash; however, strict enforcement is still lacking. The UAE National Anti-Money Laundering Committee held its Second Annual Conference in December 2004 under the title "Customs Inspectors and the Implementation of the Cash Declaration Regulation" to look at ongoing implementation efforts.

The UAE Government (UAE) also has admitted the need to better regulate "near-cash" items such as gold, jewelry, and gemstones, especially in the burgeoning markets 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 the quasi-governmental organization charged with issuing KP certificates in the UAE, and employs four individuals full-time 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 concerning the new KP requirements. UAE customs officials may delay or even confiscate diamonds entering the UAE from a KP member country without the proper certificate.

The Securities and Commodities Authority (SCA) supervises the country's two stock markets. In February 2004, it sent out anti-money laundering guidelines to brokers and the markets, instructing them to verify client information when opening accounts and created a reporting requirement for cash transactions above \$10,900. The SCA also instructed the markets and brokers to file suspicious transaction reports for initial analysis before forwarding them to the AMLSCU for further action. The instructions also provide for a five-year record keeping requirement.

Dubai's booming property market might also be susceptible to money laundering abuse. In 2002, Dubai permitted three companies to sell "freehold" properties to non-citizens. Several other emirates (though not Abu Dhabi) have announced their intention to follow suit. The intense interest in these properties, and rumors of cash purchases, sparked concerns about the potential for money laundering. As a result, developers have stopped accepting cash purchases, alleviating some of the concerns about possible money laundering activities in this sector of the economy.

The UAEG monitors registered charities in the country and requires them to keep records of donations and beneficiaries. The Ministry of Labor and Social Affairs (MLSA) regulates charitable organizations in the UAE. The CB prohibits banks from opening accounts for charities, unless they are registered with the MLSA. The UAEG is much more sensitive since September 11 to the oversight of charities and the accounting of 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.

The UAE is noted for its growing number of free trade zones (FTZs). Every emirate except Abu Dhabi has at least one functioning FTZ. There are over a hundred multinational companies located in the FTZs with thousands of 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 treated as being offshore or outside the UAE for legal purposes. However, UAE law prohibits the establishments of shell companies and trusts, and does not permit non-residents to open bank accounts in the UAE.

In March 2004, the UAEG passed Federal Law No. 8 Regarding the Financial Free Zones (Law No. 8/2004). The new law exempts FFZs and their activities from UAE federal civil and commercial laws, but subjects them and their operations to federal criminal laws including the Anti-Money Laundering Law No. 4/2002 and the Anti-Terror Law No. 1/2004. The new law and a subsequent federal decree also allowed for the establishment, in September 2004, of the UAE's first financial free zone (FFZ), known as the Dubai International Financial Center (DIFC). Sheikh Mohammed bin Rashid Al-Maktoum, Crown Prince of Dubai and UAE Defense Minister, is the President of the DIFC, which is currently the only FFZ operating in the UAE.

With regard to banking activities in the FFZs, Law No. 8/2004 limits licenses 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 free zone from dealing in UAE currency (dirham) or taking "deposits from the state's markets." It further 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 free zone and the licensing of any UAE licensed broker. The law limits any insurance activity in the UAE carried out by a free zone company, to reinsurance. It 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, the Dubai Financial Services Authority (DFSA), which reports to the office of Dubai Crown Prince and an independent Commercial Court. Observers called the independence of the DFSA into question in the summer of 2004, even prior to the inauguration of the DIFC, with the high profile firing of the chief regulator and the head of the regulatory council (the supervisory authority). Subsequent to the firing, Dubai passed laws which

appear to give the DFSA more regulatory independence from the DIFC, although these laws have not yet been tested. The DFSA, whose regulatory regime is generally modeled after the United Kingdom system, is the only authority responsible for licensing firms providing financial services in the DIFC. There are currently two banks and three other financial firms operating in the DIFC. The DFSA's rules prohibit offshore casinos or Internet gaming sites' operating in the UAE. The DFSA requires firms to send suspicious transaction reports to the AMLSCU (along with a copy to the DFSA). Although firms operating in the DIFC are subject to Law No 4/2002, the DFSA has also issued its own anti-money laundering regulations and supervisory regime, creating some ambiguity as to the authority of the CB and AMLSCU within the DIFC.

The UAE is a party to the 1988 UN Drug Convention. It signed the UN Convention against Transnational Organized Crime in 2002, but has not yet ratified it. It has yet to sign the UN International Convention for the Suppression of the Financing of Terrorism. It has entered into a series of bilateral agreements on mutual legal assistance. The CB has circulated to all financial institutions under its supervision the UNSCR 1267 Sanctions Committee's consolidated list. To date, the CB has frozen a total of \$3.13 million in 18 bank accounts in the UAE since September 11, 2001. The UAE has also frozen other financial assets under Law 4/2002. Additionally, the AMLSCU has provided international organizations and its counterpart FIUs information on cases related to terrorist financing and anti-money laundering. In April 2004, the CB Governor announced that the CB had frozen all accounts related to a company suspected of trying to smuggle nuclear materials.

The UAE was very active in supporting the creation of the Middle East and North Africa Financial Action Task Force (MENAFATF) that was inaugurated in Bahrain in November 2004; the UAE was one of the original charter signatories. MENAFATF is a FATF-style regional body. The creation of the MENAFATF is critical for pushing the region to improve the transparency and regulatory frameworks of its financial sectors.

The United Arab Emirates Government has begun constructing a far-reaching anti-money laundering program. The United Arab Emirates has sought to crack down on potential vulnerabilities in the financial markets and is cooperating in the international effort to prevent money laundering, particularly by terrorists. There has been a substantial improvement on behalf of the AMLSCU in the area of information sharing with other countries. However, there remain areas requiring further action. The Central Bank and AMLSCU should clarify and assert their jurisdiction in enforcing federal laws with respect to the DFIC. Law enforcement and customs officials should begin to take the initiative to recognize money laundering activity and proactively develop cases without waiting for referrals from the AMLSCU. United Arab Emirates officials should give greater scrutiny to trade-based money laundering in all of its forms. The Central Bank should be more diligent in its efforts to encourage hawala dealers to participate in the registration program. The AMLSCU should take a more active role in participating in international anti-money laundering gatherings and increasing its ties with other FIUs. The United Arab Emirates should ratify both the UN Convention against Transnational Organized Crime and the UN International Convention for the Suppression of the Financing of Terrorism.

## **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 drugs 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. Criminals continue to use bureaux de change, cash smuggling into and out of the UK, gatekeepers (including solicitors and accountants), and 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 the provisions of the European Union's 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 Recommendations on Money Laundering. Narcotics-related money laundering has been a criminal offense in the UK since 1986. The laundering of proceeds from other serious crimes is

criminalized by subsequent legislation. Banks and non-bank financial institutions in the UK must report suspicious transactions.

In November 2001, money laundering regulations were extended to money service bureaus (e.g., bureaux de change, money transmission companies). As of January 1, 2004, more business sectors are subject to formal suspicious transaction reporting (STR) 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 was enacted on July 24, 2002, and entered into force on January 1, 2003. The final regulations took effect on March 1, 2004. The Act creates, for the regulated sector, a new criminal offense of failing to disclose suspicious transactions in respect to all crime, not just narcotics- or terrorism-related crimes, as was the case previously. Along with the Act came an expansion of investigative powers relative to large movements of cash in the UK. In light of this, Her Majesty's (HM) Customs has increased its national priorities to include investigating the movement of cash through money exchange houses and identifying unlicensed money remitters. A total of \$159.6 million (£84 million) has been seized under the Act to date.

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 a tax advantage 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 regulated approximately 10,500 institutions and approved of 160,000 individuals in key positions (compliance officers, etc.) during the first half of 2003. 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 December 2003, the FSA fined Abbey National, the UK's sixth largest bank, \$4.37 million (£2.3 million), for "extremely serious failings" in its anti-money laundering procedures during the period 2001-2003. According to the FSA, Abbey National was cited for failure to report suspicious banking transactions in a timely manner, as well as failure to carry out proper identity checks on new customers.

STRs are filed with the Financial Intelligence Division (FID), formerly the Economic Crime Bureau, of the National Criminal Intelligence Service (NCIS), which serves as the UK's Financial Intelligence Unit (FIU). The FID analyzes reports, develops intelligence, and passes information to police forces and HM Customs and Excise for investigation. The FID received approximately 32,000 STRs in 2001, 65,000 in 2002, and 100,000 in 2003.

The Proceeds of Crime Act 2002 enhances the efficiency of the forfeiture process and increases 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 the 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.

The Terrorism (United Nations Measures) Order 2001 makes it an offense for any individual, without a license from the Treasury, 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 2004, the UK issued 20 terrorist asset freeze orders on 34 individuals and 13 organizations.

As a direct result of the events of September 11, 2001, the FID established a separate Terrorist Finance Team (TFT) to maximize the effect of reports from the regulated sector. The TFT chairs a law enforcement group to provide outreach to the financial industry concerning requirements and typologies. The operational unit that responds to the work and intelligence development of the TFT 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. This unit is now called the National Terrorist Financing Investigative Unit (NTFIU).

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 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. The UK has signed, but not yet ratified, the UN Convention against Transnational Organized Crime and the UN Convention against Corruption. The UK is a member of the FATF and the European Union. The NCIS 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 recently negotiated an asset sharing agreement that is awaiting signature by the appropriate parties. The UK also has an MLAT with the Bahamas. Additionally, there is a memorandum of understanding between the U.S. Customs Service and HM Customs and Excise.

The Government of the United Kingdom should provide adequate oversight of its gaming sector. The United Kingdom should continue the strong enforcement of its comprehensive anti-money laundering/counterterrorist financing program and its active participation in international organizations to combat the domestic and global threat of money laundering and the support and financing of terrorists and their organizations.

## **Uruguay**

In the past, Uruguay's strict bank secrecy laws, liberal currency exchange and capital mobility regulations, and overall economic stability made it a regional financial center vulnerable to money laundering. However, its extent and exact nature have always been relatively unknown. 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 likely diminished the attractiveness of Uruguayan financial institutions for money launderers in the medium term.

Uruguay has been a member of the Financial Action Task Force for South America (GAFISUD) since the organization was created in December 2000. In 2003, Uruguayan President Batlle's Deputy Chief of Staff served as the Task Force's President, and in December, 2004, Alejandro Montesdeoca

Broquetas, Uruguay's delegate to GAFISUD was selected to serve as the organization's new Executive Director Secretariat. GAFISUD's mutual evaluation in 2003 noted that Uruguay's anti-money laundering regime met international standards. GAFISUD also recognized Uruguay's efforts to train public and private sector players in money laundering-related issues.

While Uruguay's past role as a financial center put it at risk of becoming a money laundering center, the 2003 report of the OAS' Inter-American Drug Abuse Control Commission (CICAD) noted that there had been no arrests or prosecutions for money laundering in the previous three years. There were no arrests or prosecutions in 2004.

Over the last five years, the GOU has instituted several legislative and regulatory reforms in its anti-money laundering regime. In May 2001, Law 17,343 extended the predicate offenses for money laundering 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. The courts have the power to seize and confiscate property, products or financial instruments linked to money laundering activities. Legally, money laundering is considered a crime separate from underlying crimes such as narcotics-trafficking, administrative corruption, terrorism and smuggling, which are formally listed in the statutes.

In December 2003, the Uruguayan Chamber of Deputies approved a bill designed to limit bank secrecy and confidentiality. The bill is intended to increase credit transparency by eliminating bank secrecy for information pertaining to personal loans, financial credits, mortgages, or similar obligations. As of the end of 2004, however, the bill was still pending in commission in the Senate and had not been approved into law.

In its 2003 mutual evaluation report, GAFISUD made several suggestions to expand the scope of Uruguayan money laundering legislation as it relates to gambling, real estate, certain professions (primarily in the legal and financial services sectors), and the smuggling of cash and securities. GAFISUD also suggested that the Government of Uruguay (GOU) improve its investigative and administrative capabilities.

In September 2004, the Uruguayan Congress approved Law 17,835, which significantly strengthened the GOU's money laundering regime. The law incorporated all of GAFISUD's recommendations that had to be legislated, while other recommendations were met over the past two years through administrative regulations. The 2004 law expands the realm of entities subject to the filing of suspicious activities reports (SARs) and makes reporting of such activities a legal obligation. It specifically confers to the Central Bank's Financial Information and Analysis Unit (UIAF) the role of receiving and analyzing SARs, and the authority to request additional related information. The law 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.

Central Bank regulations require all banks, currency exchange houses, stockbrokers and insurance companies to implement anti-money laundering policies, such as thoroughly identifying customers, recording transactions over \$10,000 in internal databases, and reporting suspicious transactions to the UIAF. The 2004 law now makes this a legal obligation, extended to all financial intermediaries, as well as casinos, art dealers, real estate and fiduciary companies. Additionally, the law extends the reporting requirement to all persons coming in or out of Uruguay with over \$10,000 in cash or monetary instruments. Regulations for the 2004 law are being issued by the Central Bank for all entities it supervises, and by the Executive for all other reporting entities, such as casinos, real estate companies and art dealers.

Three government bodies are involved in combating money laundering. The President's Deputy Chief of Staff heads the National Drug Council, which is the senior authority directing anti-money laundering policy. The Center for Training on Money Laundering serves as a forum for discussion and policy advice based on public and private sector input. Created in 2000, the UIAF acts as a financial intelligence unit receiving, analyzing, and remitting suspicious transaction reports to judicial authorities. Central Bank Circular 1722, which created the UIAF, provides for responding to requests

for international cooperation. 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.

The Ministry of Finance and Economics, 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, which complicates efforts to track money laundering in this sector, especially in the partially foreign-owned tourist industry. The UIAF can have access to the name of titleholders at any time, however, and so can other government agencies through a judicial order. The GOU is planning to establish a computerized system that will facilitate the UIAF's access to titleholders' names.

Offshore banks are subject to the same laws and regulations as local banks, with the GOU requiring them to be licensed through a formal process that includes a background investigation. There are six offshore banks and 21 representatives of foreign banks. There are no records of the number of Uruguayan offshore firms or shell companies. 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.

Safeguarding the financial sector from money laundering is a priority for the GOU, and Uruguay remains active in international anti-money laundering efforts. It is a party to the 1988 UN Drug Convention, and participates in GAFISUD and the OAS Inter-American Drug Abuse Control Commission (CICAD) Experts Group to Control Money Laundering. The USG and the GOU are parties to extradition and mutual legal assistance treaties that entered into force in 1984 and 1994, respectively. Uruguay has signed, but not yet ratified, the UN Convention against Transnational Organized Crime. In 2003 Uruguay ratified the UN International Convention for the Suppression of the Financing of Terrorism. The GOU is taking steps to comply 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 met by the 2004 money laundering law.

Effective implementation and enforcement of its anti-money laundering legislation should be a priority for the Government of Uruguay and should enact legislation that requires the identification and registration of the titleholders of real estate- a sector that is particularly vulnerable to money laundering. Uruguay should ratify the UN Convention against Transnational Organized Crime.

## **Uzbekistan**

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

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 or automobiles, or in foreign bank accounts. The GOU could not provide information on whether financial crimes have been increasing. 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. However, drug dealers may be exchanging their drug money in a fashion that allows the black market business people to access drug dollars. It is possible that this unofficial, basically unmonitored cash-based market may create the potential for small-scale terrorist or drug-related laundering activity. The funds generated by the smuggling and corruption are not laundered through the banking system. 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 CBU, the Ministry of Finance and the state-owned and controlled banks. Although Uzbek financial institutions do not engage in illegal transactions in U.S. currency, illegal unofficial exchange houses, where the majority of cash-only money laundering takes place, deal in local soums and U.S. dollars. Moreover, drug dealers and others can transport their criminal proceeds in cash across Uzbekistan's borders for deposit in the banking systems of other countries, such as Kazakhstan, Russia or the United Arab Emirates.

Money laundering of the proceeds from drug-trafficking and other criminal activities is a criminal offense. With regard to drugs, Article 41 of the Law on Narcotic Drugs and Psychotropic substances (1999) stipulates that any institution may be closed for performing a financial transaction for the purpose of legalizing (laundering) proceeds derived from illicit narcotics-trafficking. 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. There has not yet been a complete assessment of the implementation and use of this legislation.

The CBU and the National Security Service (NSS) closely monitor all banking transactions to ensure that money laundering does not occur in the banking system. Though not legislatively mandated, 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 CBU 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 three years, possibly not sufficient time to reconstruct significant transactions. The law protects reporting individuals with respect to their cooperation with law enforcement entities. However, reportedly, the GOU has not adopted "banker negligence" laws that make individual bankers responsible if their institutions launder money.

Parliament passed a new law in August 2004 to combat money laundering and terrorist financing. This law, scheduled to take effect in January 2006, requires certain entities to report cash transactions above \$26,000 (approximately) as well as suspicious transactions. In addition, this law also covers some non-banking financial institutions, such as investment foundations, depositaries and other types of investment institutions; stock exchanges; insurers; organizations which render leasing and other financial services; organizations of postal service; pawnshops; lotteries; and notary offices. It does not include intermediaries such as lawyers, accountants, or broker/dealers. Casinos are illegal.

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.

Existing controls on transportation of currency across borders, would, in theory, facilitate detection of the international transportation of illegal source currency. When entering/exiting the country, foreigners and Uzbek citizens are required to report all currency they are carrying. Residents and non-residents may bring the equivalent of \$10,000 into the country tax-free. Amounts in excess of this limit are assessed a one-percent duty. Non-residents may take out as much currency as they brought in, however, residents are limited to the equivalent of \$2000. Residents wishing to take out higher amounts must obtain authorization to do so; amounts over \$2000 must be approved by an authorized commercial bank and amounts over \$5000 must be approved by the CBU.

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

In accordance with Uzbekistan's Code of Criminal Procedure, investigation of money laundering offenses falls under the jurisdiction of the Ministry of Internal Affairs (MVD). The Department of Investigation of Economic Crimes within the Ministry conducts investigations of all types of economic offenses. A specialized structure within the NSS and the Department on Combating Economic Crimes and Corruption in the Office of the Prosecutor General also are authorized to conduct investigations of money laundering offenses. There are no known arrests or prosecutions for money laundering or terrorist financing since January 1, 2002, except for one case following the suicide bombings of Spring 2004. 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. 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 individuals and entities included on the UN 1267 Sanction Committee's consolidated list. In addition, the GOU has circulated the lists of individuals and entities included in the U.S. executive order to the CBU, which has, in turn, forwarded these lists to all banks operating in Uzbekistan. According to the CBU, 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. We are not aware of any legislative initiatives under consideration. Although currency convertibility has been officially announced, in many regions of the country there is a strong black market for foreign exchange that accounts for a significant amount of informal economic activity.

The GOU closely monitors the activities of charitable and non-profit 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 non-profits, and the level of threat Uzbekistan itself faces from the Islamic Movement of Uzbekistan (IMU), a designated terrorist organization, 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. Major points in 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. No new legislation or changes in current law are 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 \$115,000) has been deposited into this fund since its inception, which includes about 40 million soum (\$40,000) during 2004. Roughly \$80,000 has been 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 procedure, each agency will manage the assets it seizes. There is also a specialized fund within the MVD set up 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.

Uzbekistan's government agencies are extremely cooperative and positive to efforts by the U.S. and other countries to trace or seize assets. GOU agencies make use of tips from other countries' enforcement officials regarding the flow of drug-derived assets or of assets intended to support terrorism.

The GOU has repeatedly emphasized 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 agreements with Uzbek supervisors to facilitate the exchange of supervisory information including on-site examinations of banks and trust companies operating in the country. Uzbekistan has entered into bilateral agreements for the cooperation or exchange of information on drug related issues with the U.S., Germany, Italy, Latvia, Bulgaria, Poland, China, Iran, Pakistan, the CIS, and all the countries in Central Asia. It has multilateral agreements in the framework of the CIS, under the Shanghai Cooperation Organization and under memoranda of understanding. 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 has reached informal agreement with us on mechanisms for exchanging adequate records in connection with investigations and proceedings relating to narcotics, terrorism, terrorist financing and other serious crime investigations. When requested, Uzbekistan has cooperated with appropriate law enforcement agencies of the USG and other governments investigating financial crimes and several important terrorist-related cases.

The GOU is an active party to the relevant agreements concluded under the CIS, CAEC, ECO, Shanghai Cooperation Organization and the "Six Plus Two" Group. The GOU has also participated in GUUAM (Georgia, Ukraine, Uzbekistan, Azerbaijan and Moldova) for the development of a joint law enforcement center that would cover asset seizure issues on a regional basis. Uzbekistan is a party to the 1988 UN Drug Convention, the UN International Convention for the Suppression of the Financing of Terrorism and to the UN Convention against Transnational Organized Crime.

A lack of trained personnel, resources, and modern equipment hinder Uzbekistan's efforts to fight money laundering and terrorist financing. The Government of Uzbekistan should continue to refine its pertinent legislation to bring it up to international standards. Uzbekistan also should establish supervisory oversight of intermediaries, such as accountants and attorneys, and 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. Uzbekistan should establish a Financial Intelligence Unit to receive and analyze the suspicious transaction reports it proposed to require.

## **Vanuatu**

Vanuatu's offshore sector is vulnerable to money laundering, as Vanuatu has historically maintained strict 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.

Vanuatu's financial sector includes five licensed banks (that carry on domestic and offshore business) and 60 credit unions, regulated by the Reserve Bank of Vanuatu. The Financial Services Commission (FSC) regulates the offshore sector that includes 9 banks and approximately 2,500 "international companies" (i.e., international business companies or IBCs), as well as offshore trusts and captive insurance companies. IBCs 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.

As of January 1, 2003, according to the Australian High Commission in Port Vila, the Reserve Bank of Vanuatu regulates nine offshore banks registered in Vanuatu that were formerly regulated by the FSC. This requirement 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.

The Financial Transaction Reporting Act (FTRA) of 2000 established Vanuatu's Financial Intelligence Unit (FIU) within the State Law Office. The one-person 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.

The IMFR noted several weaknesses in Vanuatu's anti-money laundering regime. Consequently, the Government of Vanuatu (GOV) has prepared a policy paper currently being considered by the Council of Ministers. FTRA amendments are expected to be passed in parliament some time this year—the next ordinary session is scheduled to sit in March. The amendments to the FTRA, if enacted, would require 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. The proposed amendments would override any inconsistent banking or other secrecy provisions and clarify the FIU's investigative powers.

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 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) retains the criminalization of the laundering of proceeds from all serious crimes, criminalizes the financing of terrorism, and includes full forfeiture, and restraining, monitoring, and production powers regarding assets.

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 continues to conduct international banking business after December 31, 2003, it will be in contravention of Section 4 of the Act, and, if found guilty, the licensee will be 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.

One of the most significant requirements of the amended legislation is the banning of "shell" banks. As of January 1, 2004, all offshore banks registered in Vanuatu must have a physical presence in Vanuatu, and management, directors, and employees must be in residence. At the September 2003 plenary session of the Asia/Pacific Group on Money Laundering (APG), Vanuatu noted its intention to draft new legislation regarding trust companies and company service providers. The new legislation will cover disclosure of information with other regulatory authorities, capital and solvency requirements, and "fit and proper" requirements. Additionally, Vanuatu is drafting legislation to comply with standards set by the International Associations of Insurance Supervisors.

The E-Business Act No. 25 of 2000 and the Interactive Gaming Act No. 16 of 2000 regulate e-commerce. Section 5 of the E-Business legislation permits the establishment of a Vanuatu-based website where business can be conducted without residency, directors, shareholders, or a registered office. Reportedly, the E-Business Act requires online operations to maintain stringent customer identification and record keeping requirements, as well as reporting suspicious transactions. The Financial Transaction Reporting Act of 2000 applies to e-commerce or businesses by defining any company listed under the Vanuatu Interactive Gaming Act 2000 as a financial institution.

In April 2002, the Organization for Economic Cooperation and Development (OECD) launched an initiative to address harmful tax practices worldwide. Vanuatu was one of seven countries listed as an "uncooperative tax haven." In January 2004, the OECD revealed that it has removed Vanuatu from its list of "uncooperative tax havens," following Vanuatu's earlier announcement that it will implement measures under the Harmful Tax Initiative. The OECD stated in a news release that it welcomes the commitment that Vanuatu has made to improve the transparency of its tax and regulatory systems, and to establish, by December 2005, effective exchange of information for tax matters with OECD countries. This move by OECD has made Vanuatu the first country to secure removal from the list of uncooperative tax havens.

In addition to the Asia Pacific Group, 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. However, Vanuatu has yet to sign either

the UN International Convention for the Suppression of the Financing of Terrorism, the UN Convention against Transnational Organized Crime, or the 1988 UN Drug Convention

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. Vanuatu should also 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 1988 UN Drug Convention.

## **Venezuela**

Venezuela is not a regional financial center, nor does it have an offshore financial sector. The relatively small but modern banking sector, which consists of 52 banks, primarily serves the domestic market. Venezuela is a major drug-transit country. Venezuela's proximity to drug producing countries, weaknesses in its anti-money laundering system, and corruption, continue to make Venezuela particularly vulnerable to money laundering. The main source of money laundering in Venezuela stems from proceeds generated by Colombia's 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 suspected 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.

The 1993 Organic Drug Law provides the only legal mechanism for the investigation and prosecution of money laundering crimes. Under this law, a direct connection between the illegal drugs and the proceeds must be proven to establish a money laundering offense. The Government of Venezuela (GOV) freezes assets of individuals charged in international drug trade or money laundering cases directly related to narcotics-trafficking. If a conviction is obtained, the frozen assets are turned over to the Ministry of Finance for use in drug demand reduction programs. After the introduction of a new Code of Criminal Procedure in 1999, responsibility for initiating these actions shifted from judges to prosecutors. Due to prosecutors' unfamiliarity with the accusatory judicial system, as well as their having to assume the burden of tens of thousands of backlogged cases, the number of cases resulting in seizure of trafficker assets has decreased.

To expand the predicate offenses for money laundering beyond activities involving the illicit drug trade, the GOV introduced the Organic Law against Organized Crime bill in 2002. Under this bill, money laundering is made a separate, autonomous offense, with no drug nexus required, and those who cannot establish the legitimacy of possessed or transferred funds, and who have awareness of the illegitimate origins of those funds, would be guilty of money laundering. The bill broadens asset forfeiture and sharing provisions, adds conspiracy as a criminal offense, strengthens due diligence requirements, establishes the Financial Intelligence Unit (FIU) as a fully autonomous unit, and provides law enforcement with stronger investigative powers by authorizing the use of modern investigative techniques such as the use of undercover agents. Although 97 of its 150 articles were approved in 2002, not a single additional article was passed in 2003 or 2004. The bill remains in its final reading at the National Assembly. If the Organized Crime bill is ultimately enacted, the GOV would meet the requirements of the 1998 Vienna Convention, the UN International Convention for the Suppression of the Financing of Terrorism, and the UN Convention against Transnational Organized Crime, all of which have been ratified by the GOV.

Under Resolution 333-97 of 1997, entitled "Standards for the Prevention, Control, and Prosecution of Money Laundering," the Superintendence of Banks and Other Financial Institutions (SUDEBAN) have implemented controls to prevent and investigate money laundering. These include stricter 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, private), savings and loan institutions, financial rental agencies, currency exchange houses, money remitters, money market funds, capitalization companies, and frontier foreign currency dealers.

The institutions are also required to file suspicious and cash transaction reports with Venezuela's FIU, the Unidad Nacional de Inteligencia Financiera (UNIF), which was created under the SUDEBAN in July 1997 and began operations in June 1998. In 2004, the UNIF was expanded to include two new divisions: one for research and development, and another for strategic analysis. Three different officials held the position of director of the UNIF in 2004.

The UNIF receives suspicious transaction reports (STRs) and reports of currency transactions exceeding 4.5 million bolívares (approximately \$2,350) from institutions regulated by SUDEBAN, 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. Some institutions regulated by SUDEBAN, such as tax collection entities and public service payroll agencies, are exempt from the reporting requirement. SUDEBAN also allows certain customers of financial institutions—those who demonstrate "habituality" in the types and amounts of transactions they conduct—to be excluded from currency transaction reports filed with the UNIF. A system has been developed for electronic receipt of currency transaction reports (CTRs), but STRs must be filed in paper format. The UNIF received 965 STRs in 2003, although that amount is expected to decrease in 2004.

In addition to STRs and CTRs, the UNIF also receives reports on the transfer of foreign currency exceeding \$10,000, the sale and purchase of foreign currency exceeding \$10,000, and summaries of cash transactions by states that exceed 4.5 million bolívares. The UNIF does not, however, receive reports on the transportation of currency or monetary instruments into or out of Venezuela. 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, including the filing of CTRs and STRs and "know your customer" policies. Each currency exchange house in the country has and employs systems to electronically transmit transaction reports to SUDEBAN and the Public Ministry. However, inadequate foreign exchange controls by the GOV's Commission for Administrative Control of Currency Exchange (CADIVI) present new opportunities to circumvent regulations applicable in the banking and financial institution sectors. Procedures to limit the potential for laundering funds through the stock market are also thought to be inadequate.

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). Approximately 30 percent of the STRs received by the UNIF are sent to the Public Ministry for further investigation. The Public Ministry 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, SUDEBAN or the Public Ministry, or by order of a Judge of Control, bank secrecy may be waived. Comprehensive financial and law enforcement information is available to the UNIF under existing legislation. When the Organized Crime bill is passed, the UNIF will become a fully autonomous unit, rather than being part of SUDEBAN. There is some concern among GOV officials about moving the UNIF out of SUDEBAN, as approximately 90 percent of the STRs received are filed by banks.

Venezuela is one of the few countries in Latin America that does not have restrictive bank secrecy laws. Although the Venezuelan constitution guarantees the right to privacy and confidentiality, investigations by the UNIF, SUDEBAN or the Public Ministry are not hindered by bank secrecy provisions. However, due to the lack of a legal basis to employ modern investigative techniques, with appropriate legal safeguards, Venezuelan law enforcement authorities find it difficult if not impossible to investigate and prosecute sophisticated criminal organizations and complex crimes such as money laundering. No law enforcement offices have dedicated specific resources to investigating and prosecuting money laundering. There is no special prosecutorial unit for the prosecution of money laundering cases under the Public Ministry, which is the only entity legally capable of initiating money laundering investigations. Currently only the drug prosecutors receive STRs from the UNIF and conduct money laundering investigations, although STRs may then be shared with other prosecutors as deemed necessary. There are only 20 drug prosecutors for all of Venezuela, most of whom lack the technical financial experience to successfully prosecute money laundering investigations, and there are no financial analysts or forensic accountants dedicated to assisting them with the preparation of their cases. Indeed, there have only been three money laundering convictions in Venezuela since 1993, and all of them were narcotics-related. No money laundering cases were tried in 2004. Venezuela has limited mechanisms for freezing assets tied to illicit activities. The assets must be

linked to a crime such as narcotics-trafficking or money laundering directly related to narcotics-trafficking, and must pass through a lengthy judicial process.

Current Venezuelan law does not specifically criminalize terrorism, although it is addressed as a matter of public order under a 1936 law. The Organized Crime Bill, when passed, would rectify this by defining terrorist activities and establishing punishments of up to 20 years in prison. The bill's expanded definition of money laundering would also make it possible to prosecute those engaged in terrorism financing, and to freeze and seize their assets. However, the bill does not establish terrorist financing as an autonomous crime.

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) Experts Group to Control Money Laundering and is a member of the Caribbean Financial Action Task Force (CFATF). Although Venezuela is a member of GAFISUD, the South American Financial Task Force, the GOV has not participated in any GAFISUD meetings or other initiatives since it first became a member in July 2003. Venezuela also participates in a multilateral initiative with the governments of the United States, Colombia, Panama, and Aruba designed to address the problem of trade-based money laundering through the Black Market Peso Exchange. Venezuela is a party to the 1988 UN Drug Convention, the UN Convention against Transnational Organized Crime, and the UN International Convention for the Suppression of the Financing of Terrorism. The GOV has signed, but not yet ratified, the UN Convention against Corruption. In January 2004, the GOV deposited its instrument of ratification for the OAS Inter-American Convention Against Terrorism. 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. The information shared has supported U.S. domestic operations, resulting in the seizure of significant amounts of money and several arrests in the United States. Venezuela has a Mutual Legal Assistance Treaty (MLAT) with the United States.

The Government of Venezuela should take steps to move forward with the passage of the Organic Law Against Organized Crime, which has been under consideration by Congress for nearly three years. The passage of this bill will provide law enforcement and judicial authorities the much-needed tools for the effective investigation and prosecution of money laundering derived from all serious crimes, and broadens assets forfeiture and sharing provisions, strengthen due diligence requirements, and expands the mandate of its Financial Intelligence Unit, the Unidad Nacional de Inteligencia Financiera (UNIF). Venezuela should also expand and strengthen the capabilities of the Public Ministry to successfully investigate and prosecute crimes related to money laundering, and provide further training to financial regulators, investigators, prosecutors and judges. Venezuela should create and enact legislation to criminalize the financing of terrorism, as well as institute measures to expedite the freezing of terrorist assets. The passage of the Organic Law Against Organized Crime and legislation criminalizing the financing of terrorism would bring Venezuela into compliance with international standards for combating financial crimes.

## **Vietnam**

The "drug economy" exists in Vietnam's informal financial system. Vietnam is a major drug producing and drug-transit country. Vietnam is not an important regional or offshore financial center. The Vietnamese banking sector is underdeveloped and the Government of Vietnam (GVN) controls the flow of all U.S. dollars in official channels. Vietnamese officials assert that their strict banking regulations prevent money laundering and terrorist financing. However, the issue is difficult to monitor since there are no laws in effect at this time to support international money laundering investigations, resulting in a lack of legal and policy-driven authority for Vietnamese law enforcement officials to cooperate bilaterally. Vietnam has a large "shadow economy" in which U.S. dollars and gold are the preferred currency. Due to the limited size of Vietnam's banking system and currency exchange controls, even legitimate businesses carry on transactions in this "shadow economy." In addition, Vietnamese regularly transfer money through gold shops and other informal mechanisms to remit or receive funds from overseas. Officially, expatriate remittances account for \$3 billion and unofficially the number may be more than double that amount.



There has been an increase in financial crimes, including but not limited to money laundering, as a result of the developing economy. Some of the transactions in both the formal and alternative remittance systems result from the proceeds of illegal narcotics sales, although the black market for smuggled goods is reportedly not significantly funded by the drug trade.

Vietnam has three free trade zones known as export processing zones (EPZ). Companies operating in EPZs manufacture goods for export and enjoy customs benefits (e.g., duty free for imported materials). A foreign invested enterprise must have a license to operate in the EPZ. The investment license often stipulates what activities the company can do or what products they can manufacture.

Vietnam does not yet have a separate law on money laundering or terrorist financing. It is working on anti-money laundering legislation, in the form of a Decree that is expected to be issued in the first quarter of 2005. The Decree is expected to cover all serious crimes without specific reference to such offenses covered in the Penal Code. However, a Decree cannot create offenses. In addition, 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 counternarcotics agency the authority to require disclosure of financial and banking records when there is a suspected violation of the law. However, the implementing regulations have not yet been promulgated. The State Bank of Vietnam, which has the lead on countering terrorist financing, can also request the disclosure of information when it believes that a transaction might fall within this category. Furthermore, the State Bank requires banks to report suspicious transactions of any kind.

Under existing Vietnamese legislation, there are provisions for seizing of assets linked to drug trafficking. In the course of its drug investigations, MPS has seized vehicles, property and cash; though the seizures typically are directly linked to the drug crime and the final confiscation requires a court finding. Reportedly, MPS can notify a bank that an account is "seized" and that is sufficient to have the account frozen.

The Asian Development Bank is working with the GVN on draft banking legislation. The GVN is also working with international financial institutions to increase its banking supervision capabilities. Currently banks are required to maintain records from seven to up to 20 years. Banks are responsible for client confidentiality but are also required to provide information to law enforcement authorities for investigation purposes. Banks are responsible for checking all identification and relevant papers presented for opening accounts and implementing transactions. Foreign currency (including notes, coins and traveler's checks) in excess of \$3,000, cash exceeding Vietnamese Dong (VND) 5,000,000 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 \$3,000 (or its equivalent in other foreign currencies) or in excess of VND 5,000,000 in cash 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 GVN is a party to the 1988 UN Drug Convention and the 1999 International Convention for the Suppression of the Financing of Terrorism. It has signed but not yet ratified the UN Convention against Transnational Organized Crime. The GVN and the USG signed a Letter Of Agreement on Counternarcotics Cooperation in December 2003, to establish and to support projects designed to combat the production and trafficking of illicit narcotics and other forms of transnational criminal activities. The GVN has circulated to its financial institutions the lists of individuals and entities that have been included on the UNSCR 1267 sanctions committee's consolidated list as being linked to Usama Bin Ladin, members of the al-Qaida organization or the Taliban, and has reported that no names or assets have been identified. Vietnamese legal provisions on counterterrorism financing are covered in various legal documents such as the Law on Credit Organizations, the Penal Code (Article 84 and Article 20. paragraph 2) and others.

The Government of Vietnam should promulgate all necessary regulations to fully implement the Counter-Narcotics Law of 2001. While it should proceed with the planned anti-money laundering decree, Vietnam should also amend its Criminal Code to create expanded terrorism offenses, as a

Decree cannot create offenses. Vietnam should establish a separate legal document governing the prevention and suppression of terrorism financing. Vietnam should ratify the UN Convention against Transnational Organized Crime. Vietnam should enforce cross border currency controls and regulate the use of gold as an alternative remittance system. Vietnam should provide implementing regulations for international cooperation regarding both drug crimes and financial crimes and improve its informal cooperation and should become a member of the Asia/Pacific Group on Money Laundering (APG).

## **Yemen**

The Yemeni financial system is not yet well developed. Thus, the extent of money laundering is not known. The prevalence of alternative remittance systems, such as hawala, makes financial institutions vulnerable to money laundering, although they are technically subject to limited monitoring by the Central Bank of Yemen (CBY). 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. But terrorism is covered in various pieces of legislation that treat terrorism and its financing as serious crimes.

Law 35 requires banks, financial institutions, and precious commodity dealers to verify the identity of persons 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 an information-gathering unit within the CBY. The unit acts as the Financial Intelligence Unit (FIU), which in turn reports to the Anti-Money Laundering Committee (AMLC). 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.

In addition, Law 35 grants the AMLC the right to exchange information with foreign entities. 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. Banks must also take every precaution when transactions appear suspicious, and report such activities to the CBY. The circular was 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 2003, U.S. Department of Homeland Security/Immigration and Customs Enforcement (DHS/ICE) agents in New York conducted an investigation of a company suspected of being involved in the smuggling and distribution of pseudoephedrine. The investigation disclosed that employees at the business were sending a large number of negotiable checks to Yemen's capital city of Sanaa. Analysis of the documents seized as a result of search warrants and bank records revealed that the suspects had also wire transferred money to an individual with suspected ties to the al-Qaida organization. ICE agents also initiated an investigation pursuant to an outbound seizure of suspected hawala-generated

funds seized en route to Yemen, concealed in jars of honey. The investigation disclosed that the courier and the reputed owner/broker of the funds were actively involved in a hawala network.

In response to the UNSCR 1267 Sanctions Committee's consolidated list and the list of Specially Designated Global Terrorists designated by the United States pursuant to E.O. 13224, and Yemen's Council of Ministers' directives, CBY issued two circulars (75304 and 75305) to all banks operating in Yemen, directing them to freeze accounts of 144 persons, companies, and organizations, and to report any finding to CBY. As a result, one account was immediately frozen. In September 2003, the CBY issued Circular No. 75304 containing a consolidated list of all persons and entities belonging to al-Qaida (182) and the Taliban (153). The Yemeni Government did not issue the circular again in 2004. 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 1, 2002, and Circular No. 91737 of November 24, 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 2004 the FIU and the CBY have been very active in enlightening 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 addition, the AMLC has prepared an anti-money laundering procedural directory that will be distributed 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). The MENAFATF is a FATF-styled regional body that promotes best practices to combat money laundering and terrorist financing in the region. It was inaugurated in November 2004 in Bahrain by 14 Arab countries. 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.

The Government of Yemen is making progress in enforcing its domestic anti-money laundering program. The passage of the 2003 anti-money laundering legislation represents a significant first step in meeting international standards. However, development of the FIU and international cooperation with criminal investigations are still in the initial development stages. The Central Bank of Yemen is still organizing its enforcement mechanism. Its effectiveness will demonstrate the authorities' commitment to ending money laundering. Yemen should also examine the prevalence of alternative remittance systems such as hawala and trade-based money laundering. As a next step, Yemen should enact specific legislation with respect to terrorist financing and forfeiture of the assets of those suspected of terrorism. It should ratify the UN Convention against Transnational Organized Crime. It should also become a party to the UN International Convention for the Suppression of the Financing of Terrorism.

## **Zambia**

Zambia is not a major financial center. To the extent that money laundering is a concern in Zambia, reports indicate that proceeds of narcotics transactions and money derived from public corruption are the major sources of laundered money. Law enforcement officials also indicate that bulk cash smuggling is a concern.

The Prohibition and Prevention of Money Laundering Act of 2001 makes money laundering a criminal offense, stiffens penalties for financial crimes, requires financial institutions to report suspicious

transactions to regulators and retain transaction records for a period of ten years, allows seizure of assets related to money laundering, and increases the investigative and prosecutorial powers of the Drug Enforcement Commission (DEC). It also establishes an Anti-Money Laundering Authority that is chaired by the attorney general and includes the heads of Zambia's principal law enforcement agencies, Revenue Authority, and Central Bank. The DEC has the responsibility for investigating money laundering offenses. When regulatory agencies have reason to suspect money laundering, they must report this to the DEC, which acts as the enforcement arm of the anti-money laundering authority, and make relevant records available to investigators. The law authorizes investigators to seize property when they have reasonable grounds to believe that it is derived from money laundering. Following a conviction under the anti-money laundering law, the court may order the forfeiture to the state of property seized during an investigation.

The anti-money laundering law does not contain specific provisions on the financing of terrorism; the Government of the Republic of Zambia (GRZ) does have the authority to order financial institutions to freeze assets, but this can be difficult if there is no evidence of a domestic crime. Zambia lacks comprehensive and reliable mechanisms for freezing the assets of terrorist organizations.

In 2003, the GRZ established an anti-money laundering unit under the DEC. The main purpose of the unit is to lead efforts within the GRZ to counter money laundering and enforce the Prevention of Money Laundering Act. In the same year, three officers of a commercial bank were tried and convicted for money laundering offenses. In 2004, the DEC conducted numerous investigations of money laundering, resulting in several arrests under the 2001 anti-money laundering statute. Trials in these cases are pending. The penalty for money laundering is imprisonment for a term not exceeding ten years and/or a fine.

In 2003, Zambia signed the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) memorandum of understanding. In 2004, Zambia's Central Bank was an active participant in ESAAMLG activities. Zambia is not a signatory to the UN International Convention for the Suppression of the Financing of Terrorism or the UN Convention against Transnational Organized Crime. Zambia is a party to the 1988 UN Drug Convention.

The Government of Zambia should establish a fully operational financial intelligence unit in accordance with international standards. Zambia should become a party to the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. Zambia should also criminalize terrorist financing and implement counterterrorist financing regulations that comport with the FATF recommendations, including the Special Recommendations on Terrorist Financing

## **Zimbabwe**

Zimbabwe is not a regional financial center and is not considered to be at significant risk for money laundering. However, it faces a serious problem with official corruption, which generates substantial funds that need to be concealed.

Narcotics-related money laundering was previously criminalized in Zimbabwe's Anti-Money Laundering Act. In 2004, the Government of Zimbabwe passed the Anti-Money Laundering and Proceeds of Crime Act. The new Act applies the anti-money laundering law to all serious offenses. It requires banks to maintain records sufficient to reconstruct individual transactions for at least six years. The 2004 Act mandates a prison sentence of up to five years for a money laundering conviction. The 2004 Act also addresses terrorist financing and authorizes the tracking and seizing of assets. Given the Government's history of using the legal system selectively and aggressively to target political opponents, the new Act has raised human rights concerns, although its use to date has not been associated with any reported due process abuses nor provoked any serious public opposition. However, the Government also has yet to make much use of the new law.

Over the past year, the Government has arrested many prominent Zimbabweans for activities it calls "financial crimes." Most of these "crimes" involve violations of currency restrictions that criminalize the externalization of foreign exchange activities conducted by many Zimbabwean businesses with

substantial volumes of imports or exports (i.e., transferring assets offshore). To date, the Anti-Money Laundering Act has not been employed in the selective prosecution of individuals for such "crimes."

When requested, the banking community has generally cooperated with the Government in the enforcement of other laws involving tracking of assets, such as laws restricting the externalization of foreign currency. The banking community and Central Bank also have cooperated with the U.S. 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 United Nations Convention against Transnational Organized Crime. 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), a FATF-style regional body, in August 2003. However, Zimbabwe has yet to sign the ESAAMLG Memorandum of Understanding (MOU).

The Government of Zimbabwe should become a party to both the UN International Convention for the Suppression of the Financing of Terrorism and the UN Convention against Transnational Organized Crime. It should sign the MOU for the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) and participate actively in that body