Chapter 2

Risks and Methods of Money Laundering and Terrorist Financing

What is Money Laundering?

Money laundering involves taking criminal proceeds and disguising their illegal source in anticipation of ultimately using the criminal proceeds to perform legal and illegal activities. Simply put, money laundering is the process of making dirty money look clean.

The Financial Action Task Force (FATF) is a Paris-based multinational or inter-governmental body formed in 1989 by the Group of Seven industrialized nations to foster international action against money laundering. According to FATF, crimes such as illegal arms sales, narcotics trafficking, smuggling and other activities of organized crime can generate huge amounts of proceeds. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits, creating the incentive to "legitimize" the ill-gotten gains through money laundering.[1]

When a criminal activity generates substantial profits, the individual or group involved must find a way to use the funds without drawing attention to the underlying activity or persons involved in generating such profits. Criminals do this by

[1] http://www.fatf-gafi.org/document/29/0,3343, en_32250379_32235720_33659613_1_1_1_1,00.html#Whatismoneylaundering.

disguising the sources, changing the form or moving the money to a place where it is less likely to attract attention.

The United Nations 2000 Convention Against Transnational Organized Crime, also known as the "Palermo Convention," defines money laundering as:[2]

- The conversion or transfer of property, knowing it is derived from a criminal offense, for the purpose of concealing or disguising its illicit origin or of assisting any person who is involved in the commission of the crime to evade the legal consequences of his actions.
- The concealment or disguising of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property knowing that it is derived from a criminal offense.
- The acquisition, possession or use of property, knowing at the time of its receipt that it was derived from a criminal offense or from participation in a crime.

One of FATF's early accomplishments was to dispel the notion that money laundering is only about cash transactions. Through its several money laundering "typologies" exercises, FATF has shown that money laundering can be achieved through virtually every medium, financial institution or business.

Another important concept in the definition of money laundering is "knowledge." In all three of the bullet points mentioned above, we see the phrase "…knowing that it is derived from a criminal offense." Generally, a broad explanation of "knowledge" is used for the definition of money laundering. FATF's 40 Recommendations on Money Laundering, its 9 Special Recommendations on Terrorist Financing and the 3rd European Union Directive on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing state that the intent and knowledge required to prove the offense of money laundering includes the concept that such a mental state may be inferred from

2 Article 6, UN Convention Against Transnational Organized Crime, 15 November 2000, http://www.unodc.org/unodc/en/treaties/CTOC/index.html.

"objective factual circumstances." In a number of jurisdictions, the term "willful blindness" is a legal principle that operates in money laundering cases. Courts define "willful blindness" as the "deliberate avoidance of knowledge of the facts" or "purposeful indifference." Courts have held that willful blindness is the equivalent of actual knowledge of the illegal source of funds or of the intentions of a customer in a money laundering transaction.

In October 2001, FATF expanded its mandate to cover the financing of terrorism. Whereas funds destined for money laundering are, by definition, derived from criminal activities, such as drug trafficking and fraud, terrorist financing may include funds from perfectly legitimate sources used to finance acts of terrorism. Concealment of funds used for terrorism is primarily designed to hide the "purpose" for which these funds are used, rather than their source. Terrorist funds may be used for operating expenses, including such things as paying for food, and rent, as well as for the actual terrorist acts. Terrorists, similar to criminal enterprises, covet secrecy of transactions and access to funds.

Both terrorists and money launderers use the same methods to move their money in ways to avoid detection, such as structuring payments to avoid reporting and underground banking, such as the ancient system of hawala.

We will discuss terrorist financing later in this chapter.

THREE STAGES IN THE MONEY LAUNDERING CYCLE

Money laundering often involves a complex series of transactions that are usually difficult to separate. However, we generally consider three phases of money laundering:

- **Step One: Placement** — The physical disposal of cash or other assets derived from criminal activity.

During this initial phase, the money launderer introduces the illegal proceeds into the financial system. Often, this is accomplished by placing the funds into circulation through financial institutions, casinos, shops and other businesses, both domestic and international. This phase can involve transactions such as:

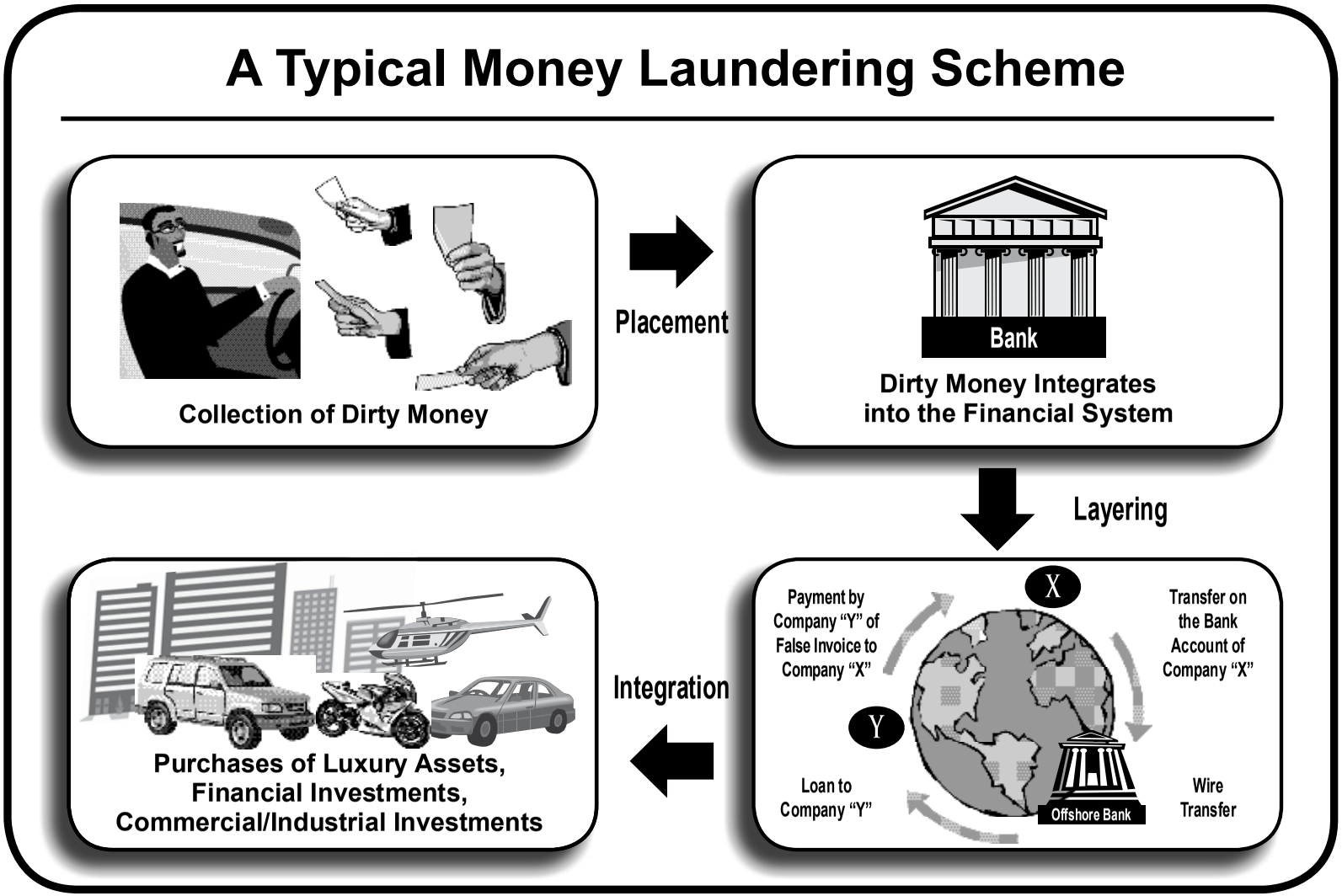
- ❑ Breaking up large amounts of cash into smaller sums and depositing them directly into a bank account.
- ❑ Transporting cash across borders to deposit in foreign financial institutions, or to buy high-value goods — such as artwork, antiques, and precious metals and stones — that can then be resold for payment by check or bank transfer.

- **Step Two: Layering** — The separation of illicit proceeds from their source by layers of financial transactions intended to conceal the origin of the proceeds.

  This second stage involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to disguise the audit trail, source and ownership of funds.

  This phase can involve transactions such as:

  - ❑ Sending wire transfers of funds from one account to another, sometimes to or from other institutions or jurisdictions.
  - ❑ Converting deposited cash into monetary instruments (e.g. traveler's checks).
  - ❑ Reselling high-value goods and prepaid access/stored value products.
  - ❑ Investing in real estate and legitimate businesses.
  - ❑ Placing money in investments such as stocks, bonds or life insurance



Source: United Nations Office on Drugs and Crime (http://www.unodc.org/unodc/en/money-laundering/laundrycycle.html)

- Using shell companies or other structures whose primary intended business purpose is to obscure the ownership of assets.

- **Step Three: Integration** — Supplying apparent legitimacy to illicit wealth through the re-entry of the funds into the economy in what appears to be normal business or personal transactions.

  This stage entails using laundered proceeds in seemingly normal transactions to create the perception of legitimacy. The launderer, for instance, might choose to invest the funds in real estate, financial ventures or luxury assets. By the integration stage, it is exceedingly difficult to distinguish between legal and illegal wealth. This stage provides a launderer the opportunity to increase his wealth with the proceeds of crime. Integration is generally difficult to spot unless there are great disparities between a person's or company's legitimate employment, business or investment ventures and a person's wealth or a company's income or assets.

THE ECONOMIC AND SOCIAL CONSEQUENCES OF MONEY LAUNDERING

The following section contains excerpts from "The consequences of money laundering and financial crime," by John McDowell and Gary Novis, which appeared in the U.S. State Department publication "Economic Perspectives" in May 2001, and from the World Bank and International Monetary Fund's "Reference Guide to Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT)." issued in January 2007.

Money laundering and terrorism financing can have potentially devastating economic, security and social consequences. While these crimes can occur in any country, they have particularly significant economic and social consequences for developing

countries, emerging markets and countries with fragile financial systems. The negative impacts of money laundering tend to be magnified in these markets because they tend to have less stable financial systems, a lack of banking regulations and effective law enforcement, and, therefore, are more susceptible to disruption from criminal or terrorism influences.

Some of the effects of money laundering and terrorist financing are:

- **Increased Crime and Corruption:** Successful money laundering helps enhance the profitable aspects of criminal activity. When a country is seen as a haven for money laundering, it will attract people who commit crime. Typically, havens for money laundering and terrorist financing have:

  - Limited number of predicate crimes for money laundering.
  - Limited types of institutions and persons covered by money laundering laws and regulations.
  - Little to no enforcement of the laws, weak penalties, or provisions that make it difficult to confiscate or freeze assets related to money laundering.

  If money laundering is prevalent, there is likely to be more corruption. Criminals may try to bribe government officials, lawyers and employees of financial or non-financial institutions so that they can continue to run their criminal businesses.

- **Undermining the Legitimate Private Sector:** One of the most serious microeconomic effects of money laundering is felt in the private sector. Money launderers are known to use front companies, or businesses that appear legitimate and engage in legitimate business, but are in fact controlled by criminals who commingle the proceeds of illicit activity with legitimate funds to hide the ill-gotten gains.

  These front companies have access to substantial illicit funds, allowing them to subsidize front company products and services at levels well below market rates. Thus, front companies have a competitive advantage over legitimate firms that draw capital funds from financial markets. This

makes it difficult for legitimate business to compete against front companies. Clearly, the management principles of these criminal enterprises are not consistent with traditional free market principles of legitimate business; thus resulting in further negative macroeconomic effects.

Finally, by using front companies and other investments in legitimate companies, money laundering proceeds can be used to control whole industries or sectors of the economy of certain countries. This increases the potential for monetary and economic instability due to the misallocation of resources from artificial distortions in asset and commodity prices. It also provides a vehicle for evading taxation, thus depriving the country of revenue.

- **Weakening Financial Institutions:** Money laundering and terrorist financing can harm the soundness of a country's financial sector. They can negatively affect the stability of individual banks or other financial institutions, such as securities firms and insurance companies. Indeed, criminal activity has been associated with a number of bank failures around the globe, including the failure of the first Internet bank, the European Union Bank, as well as Riggs Bank. Furthermore, some financial crises of the 1990s — such as the fraud and money laundering scandal at the Bank of Credit and Commerce International (BCCI) and the 1995 collapse of Barings Bank as a risky derivatives scheme carried out by a trader at a subsidiary unit unraveled — had significant criminal or fraud components. The failures in Riggs Bank's anti-money laundering controls contributed to its demise — due in large part to the manner in which Riggs Bank staff administered the accounts of, among others, Augusto Pinochet, the former President of Chile and Teodoro Obiang, the President of Equatorial Guinea.

  Financial institutions that rely on the proceeds of crime have additional challenges in adequately managing their assets, liabilities and operations. The adverse consequences of money laundering are generally described as reputational, operational, legal and concentration risks. They are interrelated, and each has financial consequences, such as:

- Loss of profitable business
- Liquidity problems through withdrawal of funds
- Termination of correspondent banking facilities
- Investigation costs and fines
- Asset seizures
- Loan losses
- Reduced stock value of financial institutions

Reputational risk is described as the potential that adverse publicity regarding an organization's business practices and associations, whether accurate or not, will cause a loss of public confidence in the integrity of the organization. As an example, for a bank, reputational risk represents the potential that borrowers, depositors and investors might stop doing business with the bank because of a money laundering scandal involving the bank. The loss of high-quality borrowers reduces profitable loans and increases the risk of the overall loan portfolio. Depositors may withdraw their funds. Moreover, funds placed on deposit with a bank may not be able to be relied upon as a source of funding once depositors learn that a bank may not be stable. Depositors may be more willing to incur large penalties rather than leaving their funds in a questionable bank, resulting in unanticipated withdrawals, causing potential liquidity problems.

FINANCIAL INSTITUTIONS THAT RELY ON THE PROCEEDS OF CRIME HAVE ADDITIONAL CHALLENGES IN ADEQUATELY MANAGING THEIR ASSETS, LIABILITIES AND OPERATIONS.

Operational risk is described as the potential for loss resulting from inadequate internal processes, personnel or systems or from external events. Such losses occur when institutions incur reduced or terminated inter-bank or correspondent banking services or an increased cost for these services. Increased borrowing or funding costs are also a component of operational risk.

Legal risk is the potential for lawsuits, adverse judgments, unenforceable contracts, fines and penalties generating losses, increased expenses for an organization, or even the closure of

the organization. For instance, legitimate customers may become victims of a financial crime, lose money and sue the organization for reimbursement. There may be investigations conducted by regulators and/or law enforcement authorities, resulting in increased costs, as well as fines and other penalties. Also, certain contracts may be unenforceable due to fraud on the part of the criminal customer.

Concentration risk is the potential for loss resulting from too much credit or loan exposure to one borrower or group of borrowers. Regulations usually restrict a bank's exposure to a single borrower or group of related borrowers. Lack of knowledge about a particular customer or who is behind the customer, or what the customer's relationship is to other borrowers, can place a bank at risk in this regard. This is particularly a concern where there are related counter-parties, connected borrowers, and a common source of income or assets for repayment. Loan losses can also result, of course, from unenforceable contracts and contracts made with fictitious persons.

For these reasons, the Basel Committee on Banking Supervision has issued statements such as the 2001 Customer Due Diligence for Banks Paper on the prevention of the criminal use of their members' banking systems by money launderers.

McDowell and Novis indicate that money laundering is critical in the effective operation of transnational and organized crime. Money laundering not only affects the Institution providing financial servicesXYZ, but also a country's economy, government and social well-being. The economic effects of money laundering include:

- **Loss of control of, or mistakes in, decisions regarding economic policy:** Due to the large amounts of money involved in the money laundering process, in some emerging market countries these illicit proceeds may dwarf government budgets, resulting in a loss of control of economic policy by governments or policy mistakes due to measurement errors in macroeconomic statistics arising from money laundering.

  Money laundering can adversely affect currencies and interest rates as launderers reinvest funds where their schemes are less likely to be detected, rather than where rates of return

are higher. Volatility in exchange and interest rates due to unanticipated cross-border transfers of funds can also be seen. To the extent that money demand appears to shift from one country to another because of money laundering — resulting in misleading monetary data — it will have adverse consequences for interest and exchange rate volatility, particularly in economies based on the US dollar, as the tracking of monetary aggregates becomes more uncertain. Last, money laundering can increase the threat of monetary instability due to the misallocation of resources from artificial distortions in asset and commodity prices.

- **Economic Distortion and Instability:** Money launderers are not primarily interested in profit generation from their investments, but, rather, in protecting their proceeds and hiding the illegal origin of the funds. Thus, they "invest" their money in activities that are not necessarily economically beneficial to the country where the funds are located. Furthermore, to the extent that money laundering and financial crime redirect funds from sound investments to low-quality investments that hide their origin, economic growth can suffer. In some countries, entire industries, such as construction and hotels, have been financed not because of actual demand, but because of the short-term interests of money launderers. When these industries no longer suit the needs of the money launderers, they abandon them, causing a collapse of these sectors and immense damage to economies that could ill-afford these losses.

- **Loss of Tax Revenue:** Of the underlying forms of illegal activity, tax evasion is, perhaps, the one with the most obvious macroeconomic impact. Money laundering diminishes government tax revenue and, therefore, indirectly harms honest taxpayers. It also makes government tax collection more difficult. This loss of revenue generally means higher tax rates than would normally be the case.

  A government revenue deficit is at the center of economic difficulties in many countries, and correcting it is the primary focus of most economic stabilization programs. The International Monetary Fund (IMF) has been involved in efforts to improve the tax collection capabilities of its member countries and the Organisaton for Economic Cooperation and

Development (OECD) has been instrumental in moving many jurisdictions towards tax transparency.

- **Risks to Privatization Efforts:** Money laundering threatens the efforts of many states trying to introduce reforms into their economies through privatization. Criminal organizations can outbid legitimate purchasers for formerly state-owned enterprises. Furthermore, while privatization initiatives are often economically beneficial, they can also serve as a vehicle to launder funds. In the past, criminals have been able to purchase marinas, resorts, casinos and other businesses to hide their illicit proceeds and to further their criminal activities.

- **Reputation Risk for the Country:** A reputation as a money laundering or terrorist financing haven could cause negative effects for development and economic growth in a country. It diminishes legitimate global opportunities because foreign financial institutions may decide to limit their transactions with institutions located in money laundering havens because the necessary extra scrutiny will make them more expensive. Legitimate businesses located in money laundering havens may suffer from reduced access to world markets (or may have to pay more to have access) due to extra scrutiny of ownership and control systems. Once a country's financial reputation is damaged, reviving it is very difficult and requires significant resources to rectify a problem that could have been prevented with proper anti-money laundering controls. Other effects include specific counter-measures that can be taken by international organizations and other countries, and reduced eligibility for governmental assistance.

- **Social Costs:** Significant social costs and risks are associated with money laundering. Money laundering is integral to maintaining the profitability of crime. It also enables drug traffickers, smugglers and other criminals to expand their operations. This drives up the cost of government expenses and budgets due to the need for increased law enforcement and other expenditures (for example, increased health care costs for treating drug addicts) to combat the serious consequences that result.

METHODS OF MONEY LAUNDERING

Money laundering is an evolving activity, and must be continuously monitored in all its various forms in order for measures against it to be timely and effective. Illicit money can move through numerous different commercial channels, including checking, savings and brokerage accounts; offshore entities and trusts; wire transfers: hawalas; securities dealers; banks; money services businesses and car dealers. As many governments around the world have implemented anti-money laundering obligations for the banking sector, there has been a shift in laundering activity from the more traditional banking sector to the non-bank financial sector and to non-financial businesses and professions.

FATF uses its annual typologies exercise to "monitor changes and better understand the underlying mechanisms of money laundering and terrorist financing." The objective is to report on some of the "key methods and trends in these areas" and to also make certain that the FATF 40 Recommendations and 9 Special Recommendations on Terrorist Financing remain effective and relevant. In this chapter, we will refer often to these typologies because they give good examples of how money can be laundered through different methods and in different settings.

BANKS AND OTHER DEPOSITORY INSTITUTIONS

Banks have historically been, and continue to be, an important mechanism for the disposal of criminal proceeds. Here are some special areas of interest and concern for money laundering through banks and other depository institutions:

ELECTRONIC TRANSFERS OF FUNDS

An electronic transfer of funds is any transfer of funds that is initiated by electronic means, such as an automated clearinghouse (ACH), computer, automated teller machine (ATM), electronic terminal, mobile phone, telephone or magnetic tape. Typically, when someone wants to rapidly move money from one bank account to another, he or she sends a wire or electronic transfer of funds. It can happen within a country or across borders, and trillions of dollars are transferred in millions of transactions each day.

Electronic funds transfer systems offer money launderers a fast conduit for moving money between countries and accounts. Illicit fund transfers are easily hidden among the millions of legitimate transfers that occur each day. Systems like Fedwire, SWIFT and CHIPS move millions of wires or transfer messages on a daily basis. Money launderers may initiate unauthorized electronic transfers of funds — such as ACH debits or by making cash advances on a stolen credit card — and place the funds into an account established to receive the transfers. This could also include stealing credit cards and using the funds to purchase merchandise, which could be sold to provide the criminal with cash. Money launderers also use electronic transfers of funds in the second phase of the laundering process, the layering cycle. The goal is to move the funds from one account to another, from one bank to another, from one jurisdiction to another, so that it becomes more difficult for law enforcement or investigative agencies to trace the origin of the funds.

To avoid detection, the money launderer may take basic precautions, such as varying the amounts sent, keeping them relatively small and, where possible, using reputable organizations.

The processes in place to verify the electronic transfer of funds, however, have been tightened. Many software providers have sophisticated algorithms to detect money laundering and other suspicious activity using electronic transfers of funds.

Some indicators of money laundering using electronic transfers of funds include:

- Funds transfers that occur to or from a financial secrecy haven, or to or from a high-risk geographic location without an apparent business reason, or when the activity is inconsistent with the customer's business or history.
- Large, incoming funds transfers that are received on behalf of a foreign client, with little or no explanation or apparent reason.
- Many small, incoming transfers of funds that are received, or deposits that are made using checks and money orders. Almost immediately, all or most of the transfers or deposits are wired to another account in a different city or country in a manner inconsistent with the customer's business or history.
- Funds activity that is unexplained, repetitive or shows unusual patterns.
- Payments or receipts are received that have no apparent link to legitimate contracts, goods or services.
- Funds transfers that are sent or received from the same person to or from different accounts.

CORRESPONDENT BANKING

The Bank of New York (BONY) scandal, which erupted in August 1999 and exposed money laundering through Russian correspondent accounts at BONY, was an early instance of laundering abuses through correspondent banking. A 305-page report, "Correspondent Banking: A Gateway to Money Laundering," issued by the United States Senate Permanent Subcommittee on Investigations, found that some large U.S. and foreign banks facilitated, through carelessness and lax procedures, the movement of diverse criminal proceeds into the U.S.

Similarly, in its Report on Money Laundering Typologies 2001-2002, FATF stated:

> Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank'"). By establishing multiple correspondent relationships globally, banks can undertake international financial transactions for themselves and for their customers in jurisdictions where they have no physical presence. Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks obtain a wide range of service through the correspondent relationship, including cash management (for example, interest bearing accounts in a variety of currencies), international wire transfers of funds, check clearing, payable-through accounts and foreign exchange services. The services offered by a correspondent bank to smaller, less well-known banks may be restricted to non-credit, cash management services. Those respondent banks judged to be sound credit risks, however, may be offered a number of credit related products (for example, letters of credit and business accounts for credit card transactions).

Correspondent banking is vulnerable to money laundering for two main reasons:

1. By their nature, correspondent banking relationships create a situation in which a financial institution carries out financial transactions on behalf of customers of another institution. This indirect relationship means that the correspondent bank provides services for individuals or entities for which it has neither verified the identities nor obtained any first-hand knowledge.

2. The amount of money that flows through correspondent accounts can pose a significant threat to financial institutions, as they process large volumes of transactions for their customers' customer. This makes it more difficult to identify the suspect transactions, as the financial institution generally does not have the information on the actual parties conducting the transaction to know whether they are unusual.

Additional risks incurred by the correspondent bank include the following issues:

- While the correspondent bank may be able to learn what laws govern the respondent bank, determining the degree and effectiveness of the supervisory regime to which the respondent is subject may be much more difficult.

- Determining the effectiveness of the respondent bank's AML controls can also be a challenge. While requesting compliance questionnaires will provide some comfort, the correspondent bank is still very reliant on the respondent doing some due diligence on the customers it allows to use the correspondent account.

- Some banks offering correspondent facilities may not ask their respondents about the extent to which they offer such facilities to other institutions ("nesting"). This adds another layer and means the correspondent bank is even further removed from knowing the identities or business activity of these sub-respondents, or even the types of financial services provided.

After decades of relatively unexamined relationships, the USA Patriot (United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act of 2001 was passed which contains several provisions concerning due diligence U.S. financial institutions needed to perform for relationships with foreign correspondent banking customers. They include:

- **Section 312**, which underscores the importance of money laundering control standards for correspondent accounts maintained for certain foreign banks. Pursuant to this section, institutions must set up risk-based due diligence to mitigate the money laundering risks posed by foreign financial institutions. In addition, for a correspondent account maintained for a foreign bank operating under an offshore license or a license

granted by a jurisdiction designated as being of concern for money laundering, a financial institution must take reasonable steps to identify the owners of the foreign bank, to conduct enhanced scrutiny of the correspondent account to guard against money laundering, and to ascertain whether the foreign bank provides correspondent accounts to other foreign banks and, if so, to conduct appropriate related due diligence.

- **Section 313**, which prohibits U.S. financial institutions from opening or maintaining correspondent accounts for foreign shell banks and requires them to take "reasonable steps" to ensure that a correspondent account of a foreign bank is not being used indirectly to provide banking services to a shell bank. A shell bank is a bank that has no physical presence in any country (a physical presence Is a place of business where the institution has at least one full-time employee, maintains operating records related to its banking activities, is subject to inspection by the banking authority that licensed it to conduct banking activities) and is not a regulated affiliate of a legitimate bank. The Senate Subcommittee report identified several cases of shell banks that facilitated millions of dollars worth of fraud schemes. In most cases, the shell banks were subject to no regulatory oversight whatsoever. As a result of the report, most countries now prohibit shell banks from operating and also prohibit their institutions from establishing relationships with shell banks.

- **Section 319** which requires U.S. financial institutions to maintain records with the names and contact information of the owners of foreign banks for which they maintain correspondent accounts. The rule also stipulates that U.S. financial institutions must keep the name and address of an agent in the U.S. designated to accept service of legal process from the U.S. government for the foreign bank's records regarding the correspondent account. For more on the

USA Patriot Act see the chapter that deals with U.S. regulatory initiatives with international ramifications.

Before establishing correspondent accounts, banks should be able to answer basic questions about the respondent bank, including who its owners are and the nature of its regulatory oversight.

Example

A lawsuit filed by a Hong Kong investor group in 2004 accused the New York branch of ABN Amro of allowing First Merchant Bank, of the Turkish Republic of Northern Cyprus, to defraud the group.

According to the lawsuit, ABN Amro ignored several warnings on six correspondent accounts it opened for First Merchant Bank at its New York branch in 1998. Soon after, the branch received two warning letters, including one from the Central Bank of Cyprus, which advised the bank of the financial and reputational risks of doing business with entities that included First Merchant. More warning letters came later, but the bank did not close the First Merchant accounts until spring 2000.

The lawsuit claimed that ABN Amro failed to conduct proper due diligence on First Merchant and its accounts and ignored a number of red flags, including:

- First Merchant held only an offshore license from Northern Cyprus;
- The bank had no physical offices except a small office in Northern Cyprus;
- It had no banking or securities licenses in New York; and
- Its chairman and managing director, Hakki Yaman Namli, was sought by Italian authorities in connection with allegedly laundering $50 million.

The bank also entered into a written agreement with the Federal Reserve, which ordered it to tighten anti-money laundering controls in its New York correspondent account and clearing service divisions.

PAYABLE-THROUGH ACCOUNTS

In some correspondent relationships, the respondent bank's own customers are permitted to conduct their own transactions — including sending wire transfers, making and withdrawing deposits and maintaining checking accounts — through the respondent bank's correspondent account without needing to clear the transactions through the respondent bank. Those arrangements are called payable-through accounts (PTAs). PTAs differ from normal correspondent accounts in that the foreign bank's customers have the ability to directly control funds at the correspondent bank. This is different from the traditional correspondent relationship, where the respondent bank will take orders from their customers and pass them on to the correspondent bank. In these cases, the respondent bank has the ability to perform some level of oversight prior to executing the transaction.

PTAs can have a virtually unlimited number of sub-account holders, including individuals, commercial businesses, finance companies, exchange houses or casas de cambio, and even other foreign banks. The services offered to the "subaccount holders" and the terms of the PTAs are specified in the agreement signed by the correspondent and the respondent banks.

PTA accounts held in the names of respondent banks often involve checks encoded with that bank's account number and a numeric code to identify the sub-account, which is the account of the respondent bank's customer. Sometimes the sub-account holders are not identified to the correspondent bank.

Elements of a PTA relationship that can threaten the correspondent bank's money laundering defenses include:

- PTAs with foreign institutions licensed in offshore financial services sectors with weak or absent bank supervision and weak licensing laws.
- PTA arrangements where the correspondent bank regards the respondent bank as its sole customer and fails to apply its Customer Due Diligence policies and procedures to the customers of the respondent bank.
- PTA arrangements in which sub-account holders have currency deposit and withdrawal privileges.
- PTAs used in conjunction with a subsidiary, representative or other office of the respondent bank, which may enable the respondent bank to offer the same services as a branch without being subject to supervision.

Example

Lombard Bank — a bank licensed by the South Pacific island of Vanuatu, which is considered by many experts as a tax and money laundering haven — opened a payable-through account at American Express Bank International (AEBI) in Miami. The Vanuatu bank offered its Central American customers virtually full banking services through its payable-through account at AEBI. The customers were given checkbooks allowing them to deposit and withdraw funds from Lombard's payable-through account. Lombard was permitted to have multiple authorized signatures on the account. The Lombard customers had no relationship with AEBI. The sub-account holders would bring cash deposits to Lombard representatives in four Central American countries. Lombard couriers would transport the cash to its Miami affiliate, Lombard Credit Corporation, for deposit in the payable-through account at AEBI. Lombard customers also brought cash to the Lombard office in Miami, which was located in the same building as AEBI. That cash also was deposited in the payable-

through account at AEBI. Over two years, ending June 1993, as much as $200,000 in cash was received by Lombard's Miami affiliate on 104 occasions.

CONCENTRATION ACCOUNTS

Concentration accounts are internal accounts established to facilitate the processing and settlement of multiple or individual customer transactions within the bank, usually on the same day. These accounts are also known as special-use, omnibus, settlement, suspense, intraday, sweep or collection accounts. Concentration accounts are frequently used to facilitate transactions for private banking, trust and custody accounts, funds transfers and international affiliates.

Example

Vladimiro Montesinos, former spymaster and henchman of Peruvian ex-President Alberto Fujimori, held at least two accounts, including a "concentration" account, in his own name at the Bank of New York, which he used to funnel money to recipients of his corrupt largesse while he served as Peru's intelligence chief.

Money laundering risks can arise in concentration accounts if the customer-identifying information, such as name, transaction amount and account number, is separated from the financial transaction. If separation occurs, the audit trail is lost, and accounts may be misused or administered improperly. Banks that use concentration accounts should implement adequate policies, procedures and processes covering operation and recordkeeping for these accounts.

Here are some anti-money laundering practices for these accounts.

- Requiring dual signatures on general ledger tickets.
- Prohibiting direct customer access to concentration accounts.

- Capturing customer transactions in the customer's account statements.
- Prohibiting customers' knowledge of concentration accounts or their ability to direct employees to conduct transactions through the accounts.
- Retaining appropriate transaction and customer identifying information.
- Reconciling accounts frequently by an individual who is independent from the transactions.
- Establishing a timely discrepancy resolution process.
- Identifying and monitoring recurring customer names.

PRIVATE BANKING

Private banking is an extremely lucrative, competitive and worldwide industry and is an important issue when discussing the money laundering field. In the early 1990s, private banking received unwanted publicity from the scandal surrounding the movement of hundreds of millions of dollars of purportedly ill-gotten money belonging to Raul Salinas, the brother of former Mexican President Carlos Salinas. His fortune, in large measure, was handled by private bankers employed by Citibank in Mexico City, New York, London and Geneva.

Private banking provides highly personalized and confidential products and services to well-heeled clients at fees that are often based on "assets under management." Private banking often operates semi-autonomously from other parts of a bank and caters to wealthy customers who seek confidentiality and personalized service.

Fierce competition among private bankers for the high net-worth individuals who are their main clientele has given rise to the need for tighter government controls worldwide. Competition brings increased pressures on the relationship managers and the marketing officers to obtain new clients, to increase their assets under management, and to contribute a greater percentage to the

net income of their organizations. Plus, the compensation paid to most "relationship managers" in private banking is based largely on the assets under management that they bring to their institutions.

Examples

In the United States, in the case of American Express Bank International (AEBI), two private bankers formerly employed by AEBI were convicted of money laundering. They cited the competitive nature of the field, the method of compensation and "the pressure on international bankers to recruit new clients and the concomitant professional and monetary success that comes to those who are able to produce."

In the United States, Riggs Bank maintained a close relationship with Augusto Pinochet, the former President of Chile. This relationship with Pinochet, included flying to and from Chile on his private jet and taking hundreds of thousands of dollars worth of cashiers checks to Pinochet, which later were found to be the proceeds of corruption. Riggs also facilitated the movement of money through real estate transactions that appeared to be structured in such a way as to avoid linking them to Pinochet. Riggs Bank, which was a well-respected bank founded in the 1800s, was fined millions of dollars for violations of the U.S. Bank Secrecy Act.

The following factors may contribute to the vulnerabilities of private banking with regard to money laundering:

- Perceived high profitability.
- Intense competition.
- Powerful clientele.
- The high level of confidentiality associated with private banking.

- The close relationship of trust developed between relationship managers and their clients.
- Commission-based compensation for relationship managers.
- A culture of secrecy and discretion developed by the relationship managers for their clients.
- The relationship managers becoming client advocates to protect their clients.

Often, private banking customers are "non-resident aliens" meaning they are conducting their banking in a country outside the one in which they reside. Their assets may move overseas where they are held in the name of corporations established in secrecy havens. Private investment companies (PICs), which have been an element of many high-profile laundering cases in recent years, are excellent laundering vehicles. PICs are corporations established by individual bank customers and others in offshore jurisdictions to hold assets. They are "shell companies" formed to maintain clients' confidentiality and for various tax- or trust-related reasons. The secrecy laws of the offshore havens where PICs are often established can conceal the true identity of their beneficial owners. As an additional layer of secrecy, some PICs will be established with nominal owners, who hold title to the company for the benefit of individuals who remain undisclosed and sometimes subject to an attorney-client privilege or other similar legal safeguards. Many private banks establish PICs for their clients, often through an affiliated trust company in an offshore secrecy haven.

Another area of concern with regard to private banking includes corrupt "Politically Exposed Persons" (PEPs). PEPs have been the source of problems for some financial institutions, as set forth in the examples below.

Examples

- Mario Villanueva, the corrupt governor of the Mexican state of Quintana Roo, according to the U.S. Drug Enforcement Agency, facilitated the smuggling of 200

tons of cocaine into the U.S. For five years, until 2001, he maintained private banking accounts at Lehman Brothers containing approximately $20 million that the DEA alleged he had received as bribes from Mexican drug traffickers.

- The Riggs Bank case revealed a web of transactions, involving hundreds of millions of dollars, that the bank had facilitated over many years for dictators on two continents, including Augusto Pinochet of Chile and Teodoro Obiang of Equatorial Guinea. The accounts formed part of the embassy banking portfolio that was the bank's specialty product for decades.

- Vladimiro Montesinos, the former head of Peru's Intelligence Service, and chief advisor of former Peruvian president Alberto Fujimori, had accounts at The Bank of New York, in New York City, which held his substantial bribes from drug traffickers. Other institutions, such as American Express Bank International, Bank of America, Barclays and UBS AG, in New York, also held accounts for Montesinos.

- Arnoldo Aleman and Byron Jerez, the former president and tax commissioner, respectively, of Nicaragua, maintained accounts at Terrabank N.A. in Miami, through which they bought millions of dollars of certificates of deposit and condominiums in South Florida, allegedly with the proceeds of corruption.

- Pavel Lazarenko, the former prime minister of Ukraine, had accounts in San Francisco at Bank of America, Commercial Bank, Pacific Bank, WestAmerica Bank, and various securities firms, including Fleet Boston, Robertson & Stephens, Hambrecht & Quist and Merrill Lynch, where millions of dollars he allegedly extorted as head of state of Ukraine were held.

- Colonel Victor Venero Garrido, a Peruvian army officer, whom the U.S. FBI described as the "most trusted bag/straw man" of Vladimiro Montesinos, maintained

accounts at Citibank in Miami and Northern Trust in California that allegedly held more than $15 million in bribes and extortion proceeds.

- Mario Ruiz Massieu, the former deputy attorney general of Mexico in charge of drug trafficking prosecutions maintained a private banking account at Texas Commerce Bank in Houston in the mid-1990s, where he deposited drug traffickers' bribes of $9 million in currency over a 13-month period.

STRUCTURING

Designing a transaction to evade triggering a reporting or recordkeeping requirement is called "structuring." Structuring is possibly the most commonly known money laundering method. It is a crime in many countries, and must be reported by filing a suspicious transaction report. The individuals engaged in structuring are runners, hired by the launderers. These individuals go from bank to bank depositing cash and purchasing monetary instruments in amounts under the reporting threshold.

Structuring can be done in many settings or industries, including banking, money services businessess and casinos.

Examples

- **A customer breaks a large transaction into two or more smaller ones.**

  Henri wants to conduct a transaction involving €18,000 in cash. However, knowing that depositing it all at once would exceed the cash reporting threshold and would trigger the filing of a report, he goes to three different banks and deposits €6,000 in each.

- **A large transaction is broken into two or more smaller transactions conducted by two or more people.**

Jennifer wants to send a €5,000 money transfer, but knowing that, in her country, there is a threshold of €3,000 for recording of funds transfers which would be triggered, she sends a €2,500 money transfer and asks her friend to send another €2,500 money transfer.

- **Real-life case:** Isaac Kattan was a travel agent and businessman. Kattan allegedly laundered an estimated $500 million per year in drug money, all of it in cash. Couriers from a number of cities would visit him in his apartment, leaving boxes and suitcases full of money. The bagmen were messengers from narcotics distributors. The money was payment to their suppliers in Colombia. One of Kattan's favorite places for making deposits was The Great American Bank of Dade County. Officials in the bank were bribed to accept his massive deposits without filing currency transaction reports (CTRs). Hernan Botero, another individual, allegedly had a similar operation which was smaller than Kattan's. He laundered only about $100 million per year out of his home near Palm Beach. The Botero group used offshore corporations to invest in Florida real estate as another way to launder money from cocaine deals. Botero was indicted in the United States and testimony in federal court showed he had bribed officers and employees of the Landmark Bank in Plantation, Florida, to accept his deposits. The money was brought in almost daily by Botero front companies. From Landmark, the money was transferred to the Miami accounts of Colombian banks. From there, it was a simple matter to wire the money to banks in Colombia. By the early 1980s, the federal Operation Greenback had arrested Kattan, Botero, and others. Kattan and Botero were sentenced to 30-year terms in federal prison.

Here is how foreign "money brokers" conduct what is called structuring:

- A structurer, who is acting for a foreign money broker, opens numerous checking accounts in Country A using real and fictitious names. Sometimes the structurer uses identification documents of dead people supplied by the money brokers.
- With funds supplied by the money brokers, the structurer opens the accounts with inconspicuous amounts, usually in the low four-figures.
- To allay bank suspicions, the money brokers sometimes deposit extra funds to cover living expenses and to give the accounts an air of legitimacy.
- Once the accounts are opened, the structurer signs the newly-issued checks in blank, leaving the payee, date and amount lines blank.
- He sends the signed blank checks to the money broker in country B, usually by courier.
- A structurer may open as many as two dozen checking accounts in this fashion. It is not uncommon for brokers to have more than 20 of these checking accounts in Country A available at any given time.
- The checking accounts usually accumulate only a few thousand dollars before they are cleared out by checks drawn by the money brokers to pay for exports from Country A to Country B's money brokerage customers.
- The availability of hundreds of these accounts to Country B's money brokers leaves open the possibility that tens of millions of dollars could be passing through them each year.

In 2005, FATF added a new term to the vast money laundering lexicon – "cuckoo smurfing."

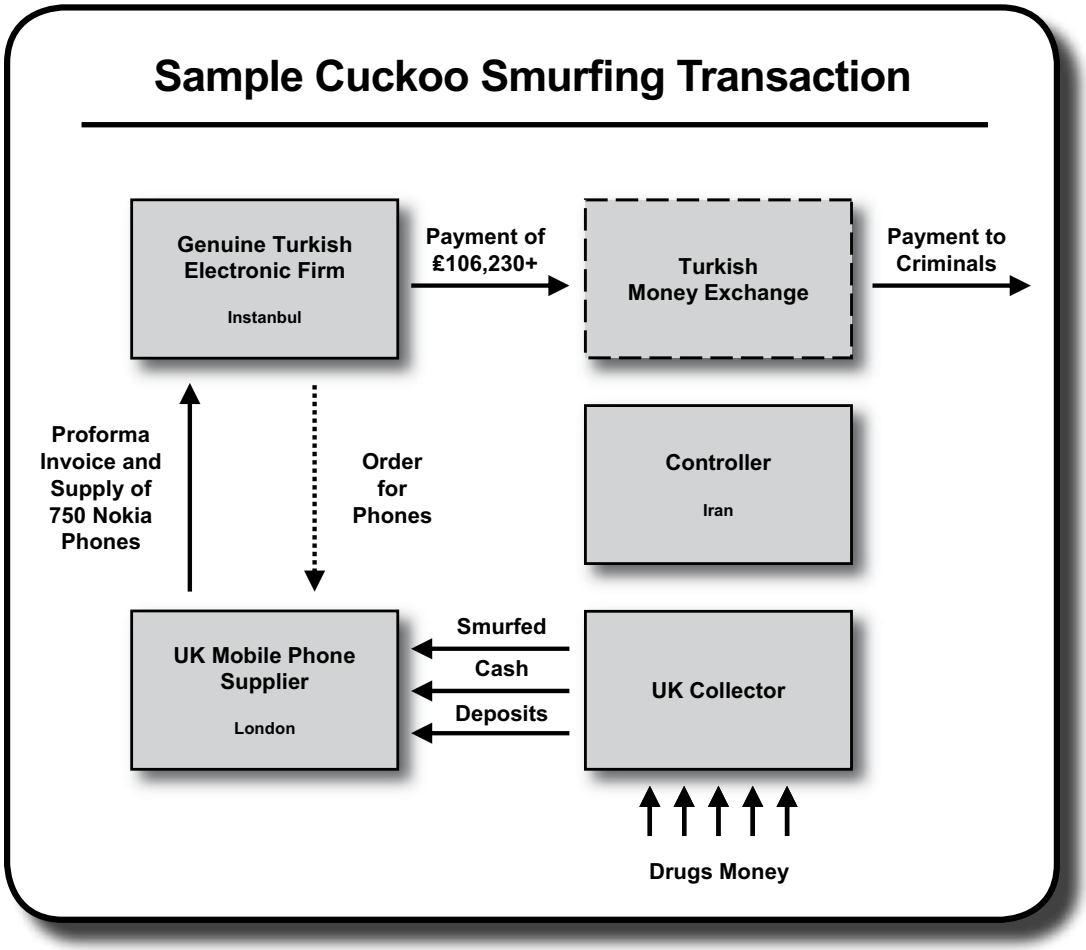
The term, mentioned in the organization's 2005 Typologies Report, refers to a form of money laundering linked to alternative remittance systems, in which criminal funds are transferred through the accounts of unwitting persons who are expecting genuine funds or payments from overseas. The term cuckoo smurfing first originated in investigations in the United Kingdom, where it is a significant money laundering technique.

The cuckoo is a European bird that is a parasite because it lays its eggs in the nests of other birds, which hatch them and rear the offspring. The main difference between traditional structurer and cuckoo smurfing is that in the latter the third parties who hold the bank accounts being used are not aware of the fact that illicit money is being deposited into their accounts.

Cuckoo smurfing requires the work of an insider within a financial institution and is generally a four step process:

- The first step occurs when a customer provides funds to an alternative remitter for transfer to a beneficiary, generally in another country.
- The next step involves the insider, who will provide the transaction details (beneficiary name, bank, account number and amount) of the transfer to an associate in the foreign country where the beneficiary of the transfer is located. The associate in the foreign country will have cash that needs to be placed into the financial system.
- The associate in the foreign country will then deposit cash into the bank account of the intended beneficiary. The beneficiary will receive the full amount of the transfer and the associate in the foreign country will be able to place some of its cash into the financial system.
- The associate in the foreign country then arranges to get the funds from the alternate remitter, using one of the methods by which alternate remitters transfer funds. In this case, the associate in the foreign country will have laundered the funds and will have legitimate funds to replace the criminally derived ones deposited into the beneficiary's account.

- To combat cuckoo smurfing, FATF recommends that banks have controls in place to identify depositors who pay cash into third-party accounts. Also, banks should monitor for unusual cash deposits that are structured or placed in branches other than where the customer's account is held.



Source: Financial Action Task Force Report on Money Laundering Typologies 2004 - 2005 (http://www.fatf-gafi.org/dataoecd/16/8/35003256.pdf).

According to FATF, the following should be kept in mind when dealing with possible cuckoo smurfing activity:

- The existence of these deposits is not necessarily grounds to reconsider the relationship with a customer.
- It could be the indicator of laundering, therefore it should be examined carefully.

- Law enforcement will need information on the depositor, so banks should seek to identify cash deposits made by third parties and should retain surveillance footage.

Another form of placing large amounts of cash into the financial system is called microstructuring. Microstructuring is essentially the same as structuring, except that it is done at a much smaller level. Instead of taking $18,000 and breaking it into two deposits, the microstructurer might break it into 20 deposits of approximately $900 each. This level of structuring makes it extremely difficult to detect. In the case of a Colombian drug cartel, the cash proceeds of U.S. drug sales are deposited into accounts in New York. These accounts have an ATM card linked to them. The card is provided to associates in Colombia. The deposits are made on a regular schedule, which is communicated by the U.S. microstructurer to the Colombian associates. The Colombian associates withdraw the funds, as they are deposited, in Colombian pesos and provide them to the drug lords. In one case in New York, an individual was trailed by law enforcement authorities as he went from bank to bank in Manhattan. When they stopped him, he had $165,000 in cash.

A few means of detecting microstructuring include:

- Use of counter deposit slips as opposed to preprinted deposit slips.
- Frequent activity in an account immediately following the opening of the account with only preliminary and incomplete documentation.
- Frequent visits to make cash deposits of nominal amounts that are inconsistent with typical business or personal banking activity.
- Cash deposits followed by ATM withdrawals, particularly in higher risk countries.
- Cash deposits made into business accounts by third parties with no apparent connection to the company.

BANK COMPLICITY

A criminally co-opted bank employee might facilitate money laundering. Institutions and businesses have learned that an insider can pose the same money laundering threat as a customer. It has become part of the mantra in the anti-money laundering field that it is essential to maintain co-equal programs to know your customer and to know your employee.

In an effort to identify and anticipate trouble before it costs time, money and reputation, companies are developing programs to look closely at the people working inside their own four walls. Knowing your employee is as crucial to a company's security as knowing customers and other "outsiders." (See also the section on AML Compliance Programs.)

Example

In 2000, Lucy Edwards, a former vice president of Bank of New York's Eastern European Division, and her husband, Peter Berlin, pled guilty in New York federal court to a money laundering conspiracy linked to facilitating the movement of hundreds of millions of dollars of dubious origin from Russia through corporate accounts Berlin had opened at the bank.

While background screening of prospective and current employees, especially for criminal history, can keep unwanted employees out and can identify those to be removed, institutions need ongoing controls to help identify those employees who may be actively committing crimes against their employers. In this case, it is critical to have solid internal controls, such as ensuring that Customer Due Diligence files are complete, having suspicious activity monitoring alerts carefully reviewed when they continue to arise in the portfolio of a particular account officer, and understanding customer and employee relationships. (Peter Berlin, Lucy Edwards' husband, was one of her largest clients - a conflict of interest such as this should trigger a closer review of the relationship.)

CREDIT UNIONS OR BUILDING SOCIETIES

The United Kingdom's Joint Money Laundering Steering Group (JMLSG) stated in a November 2006 guidance that, although credit unions pose a low money laundering risk, they are still vulnerable to money laundering and terrorist financing schemes. In the 2007 update, the JMLSG included credit unions and building societies in the scope of its recommendations to have AML programs in place. On the plus side, their relatively small size, compared to banks and other financial institutions, makes it harder for criminals to launder illicit cash because suspicious activity can be more easily discovered within a smaller volume of transactions, the JMLSG report found.

Not surprisingly, the more financial services a credit union offers, the higher the potential risk for money laundering, as these credit unions tend to contain a larger clientele and offer potential criminals a larger range of possible ways to conceal their illicit funds. Overall, though, credit unions contain "high levels of cash transactions," which increases the risk of money laundering and terrorist financing.

The group concluded that other high-risk transactions include: money transfers to third parties, third parties paying in cash for someone else and reluctance to provide identity information when opening an account.

The JMLSG even advised credit unions to watch for unusual activity in the accounts of children because parents could be trying to use those funds for illicit purposes, thinking such transactions would draw less attention.

NON-BANK FINANCIAL INSTITUTIONS

CREDIT CARD INDUSTRY

The credit card industry includes:

- Credit card associations, such as American Express, MasterCard and Visa, which license member banks to issue bankcards, authorize merchants to accept those cards, or both
- Issuing banks, which solicit potential customers and issue the credit cards.
- Acquiring banks, which process transactions for merchants who accept credit cards.
- Third-party processors, which contract with issuing or acquiring banks to provide transaction processing and other credit card–related services for the banks.

Credit card accounts are not likely to be used in the initial placement stage of money laundering because the industry generally restricts cash payments. They are more likely to be used in the layering or integration stages.

Example

Money launderer Josh prepays his credit card using illicit funds that he has already introduced into the banking system, creating a credit balance on his account. Josh then requests a credit refund, which enables him to further obscure the origin of the funds, which constitutes layering. Josh then uses the illicit money he placed in his bank account and the credit card refund to pay for a new kitchen that he bought. Through these steps he has integrated his illicit funds into the financial system.

A money launderer could put ill-gotten funds in accounts at banks offshore and then access these funds using credit and debit

cards associated with the offshore account. Alternatively, he could smuggle the cash out of one country into an offshore jurisdiction with lax regulatory oversight, place the cash in offshore banks and — again — access the illicit funds using credit or debit cards.

In a 2002 Report called "Extent of Money Laundering through Credit Cards Is Unknown," the U.S. Government Accountability Office, the Congressional watchdog of the United States, offered hypothetical money laundering scenarios using credit cards. One example was: "[Money launderers establish a legitimate business in the U.S. as a 'front' for their illicit activity. They establish a bank account with a U.S.-based bank and obtain credit cards and ATM cards under the name of the 'front business.' Funds from their illicit activities are deposited into the bank account in the United States. While in another country, where their U.S.-based bank has affiliates, they make withdrawals from their U.S. bank account, using credit cards and ATM cards. Money is deposited by one of their cohorts in the U.S. and is transferred to pay off the credit card loan or even prepay the credit card. The bank's online services make it possible to transfer funds between checking and credit card accounts."

MONEY REMITTERS AND MONEY EXCHANGE HOUSES

Money remitters transfer funds for their customers. They receive cash from their clients which is transferred to designated beneficiaries against payment of a commission. These businesses provide a valid and legitimate financial service.

The industry is popular with many individuals who do not have real access to formal banking services and because money remitters often charge lower commission rates than banks for transferring money abroad. Funds are often transferred to the least advanced regions of the world, where no formal banking services exist.

In its report on money laundering typologies of 1996-1997, FATF stated that this industry operated in a variety of ways, but most commonly a money remitter receives cash which it transfers through the banking system to another account held by an

associated company in the foreign jurisdiction, where the money is made available to the ultimate recipient.

The different operations can be classified as follows:

- Funds transfer companies possessing separate networks (Western Union and Money Gram).
- Money transfer systems connected with informal banking channels or underground banking. (This type of banking will be described in greater detail in the section on terrorist financing.)
- Money transfers by way of the collection accounts of foreign banks (accounts opened with subsidiaries or branches, or even representative offices of foreign banks, which transfer the earnings of immigrant or visiting workers to their countries of origin).
- International money orders.

Like banks, remittance services have been widely used for money laundering. The risks of laundering are not confined to the informal funds transfer networks; they may also apply to official networks like those of the government postal service. The 1997-1998 FATF report on money laundering typologies stated that the authorities of a Scandinavian country had noticed a steep increase in international money orders to the countries of the former Yugoslavia. In a FATF member country, the mail was reported to have been used to send packages containing large cash sums and drugs anonymously.

The biggest misconception about this industry is that there is minimal oversight. In fact, many are subject to a variety of national and/or local regulators and often have extremely tight compliance programs in place. The scrutiny to which money remitters are subject can vary greatly, in large part due to the ease with which some money transmitters can set up their business and not be subject to any regulation. This is why one of the most important aspects of due diligence for a bank when establishing a relationship with a money transmitter is to confirm that the customer is properly licensed.

Another technique commonly used by money launderers using money remitters and currency exchanges is for the broker to make the funds available to the criminal organization at the destination country in the local currency. The launderer/broker then sells the criminal dollars to foreign businessmen wishing to make legitimate purchases of goods for export. This correspondent type operation resembles certain aspects of "underground remittance services," which will be discussed more in the section on terrorist financing.

Cash proceeds from criminal activities can also transit through the money exchange sector. Here is an example from the 1997-1998 FATF Report on Money Laundering Typologies of suspicious activity in a money exchange setting:

Example

A bureau de change ("The Counter") had been doing business in a small town near the German border for a number of years before exchange offices became regulated within the country and transactions became subject to reporting obligations to prevent money laundering. The Counter often had a surplus of high denomination bank notes. The owner (Peter) knew these notes were not popular and, therefore, had them exchanged into smaller denomination notes at a nearby bank. Before the legislation took effect, persons acting on behalf of The Counter regularly exchanged amounts in excess of US$ 50,000 in value, but immediately after the legislation took effect, the transactions were reduced to amounts of US$ 15,000 to US$ 30,000 per transaction in an attempt to structure the exchanges so that they were under the transaction reporting threshold. The employees of the bank branch regarded the exchanges, which did not have any sound economic reason, as dubious and reported the transactions.

Peter had a record with the police related to fencing stolen property and dealing in drugs, and because of this he transferred ownership of The Counter to a new owner named Andre with no police record. Andre registered The Counter with the Central Bank as an

ANOTHER TECHNIQUE COMMONLY USED BY MONEY REMITTERS AND CURRENCY EXCHANGES IS FOR THE BROKER TO MAKE THE FUNDS AVAILABLE TO THE CRIMINAL ORGANIZATION AT THE DESTINATION COUNTRY IN THE LOCAL CURRENCY.

exchange office and was accepted on a temporary basis. The financial intelligence unit consulted various police files and established that the police had been observing this exchange office for some time. The suspect transactions were passed on to the crime squad in the town where The Counter had its office, and the crime squad started an investigation. A few months later, the crime squad arrested Andre, house searches were conducted, resulting in the seizure of expensive objects and an amount equivalent to more than US$ 250,000 in cash. The records of The Counter showed that many transactions were not recorded in the official books and records. For example, over a period of thirteen months, The Counter changed the equivalent of more than US$ 50 million at a foreign bank without registering these exchange transactions in the official books and records. The investigation showed that The Counter and its owners were working with a group of drug traffickers, who used the exchange office to launder their proceeds, and this formed a substantial part of the turnover of the business.

This case underscored the need for banks and large, legitimate bureaux de change to pay attention to their business relations with smaller bureaux, particularly when supplying or exchanging currency.

INSURANCE COMPANIES

In its 2002-2003 typologies report, FATF experts submitted case examples that showed the vulnerabilities of the insurance sector to money laundering. The primary emphasis in the examples was on the investment aspect of life insurance policies. Most significant laundering and terrorist financing risks in the insurance industry are found in life insurance and annuities products. While many life insurance policies are generally structured to pay a certain sum upon the death of the insured, others have an investment value which can create a cash value if the policyholder wishes to cancel the policy. Life insurance policies that have an investment feature, which can increase the death benefit as well as the cash value of the policy, are often referred to as whole life or permanent life.

MOST SIGNIFICANT LAUNDERING AND TERRORIST FINANCING RISKS IN THE INSURANCE INDUSTRY ARE FOUND IN LIFE INSURANCE AND ANNUITIES PRODUCTS.

Annuities are another type of insurance policy that has a cash value. An annuity is an investment that provides a defined series of payments in the future in exchange for an up-front sum of money. Annuity contracts may allow criminals to exchange illicit funds for an immediate or deferred income stream, which usually arrives in the form of monthly payments starting on a specified date. One indicator of possible money laundering is when a potential policyholder is more interested in a policy's cancellation terms than its benefits. In both cases, a policyholder can place a large sum of money into a policy with the expectation that it will grow based on the underlying investment, which can be fixed or variable. In a number of ways, the sector's susceptibility to money laundering is similar to that of the securities sector. For example, in some jurisdictions, life insurance policies are viewed as an investment vehicle similar to securities. We will discuss the securities industry in the next section.

In contrast to life insurance and annuities, policies for property insurance, casualty, title or health insurance typically do not offer investment features, cash build-ups, the option of transferring funds from one to another, or other means of hiding or moving money.

Vulnerabilities in the insurance sector include:

- Lack of oversight/controls over intermediaries: Insurance brokers have a great deal of control and freedom regarding policies.
- Decentralized oversight over aspects of the sales force: Insurance companies may have employees (captive agents) who are subject to the full control of the insurance company. Non-captive agents, those who offer an insurance company's products, but are not employed by an insurance company (i.e., the non-captive agent will often work with several insurance companies to find the best mix of products for their clients) may fall between the cracks of multiple insurance companies or may work to find the company with the weakest AML oversight if they are complicit with the money launderer.

- Sales-driven objectives: The focus of brokers is on selling the insurance products and, thus, they often overlook signs of money laundering, such as a lack of explanation for wealth or unusual methods for paying insurance premiums.

Examples of how money can be laundered through the insurance industry include:

- Certain insurance policies operate in the same manner as unit trusts or mutual funds. The customer can over-fund the policy and move funds into and out of the policy while paying early withdrawal penalties. When such funds are reimbursed by the insurance company (by check, for example), the launderer has successfully obscured the link between the crime and the generated funds.

- The purchase and redemption of single premium insurance bonds are key laundering vehicles. The bonds can be purchased from insurance companies and then redeemed prior to their full term at a discount. In such cases, the balance of the bond is paid to a launderer in the form of a “sanitized” check from the insurance company.

- Use of the free-look period: A free-look period is a feature that allows investors, for a short period of time after the policy is signed and the premium paid, to back out of a policy without penalty. This process allows the money launderer to get an insurance check, which represents cleaned funds. However, as more insurance companies are subject to AML program requirements, this type of money laundering is more readily detected and reported.

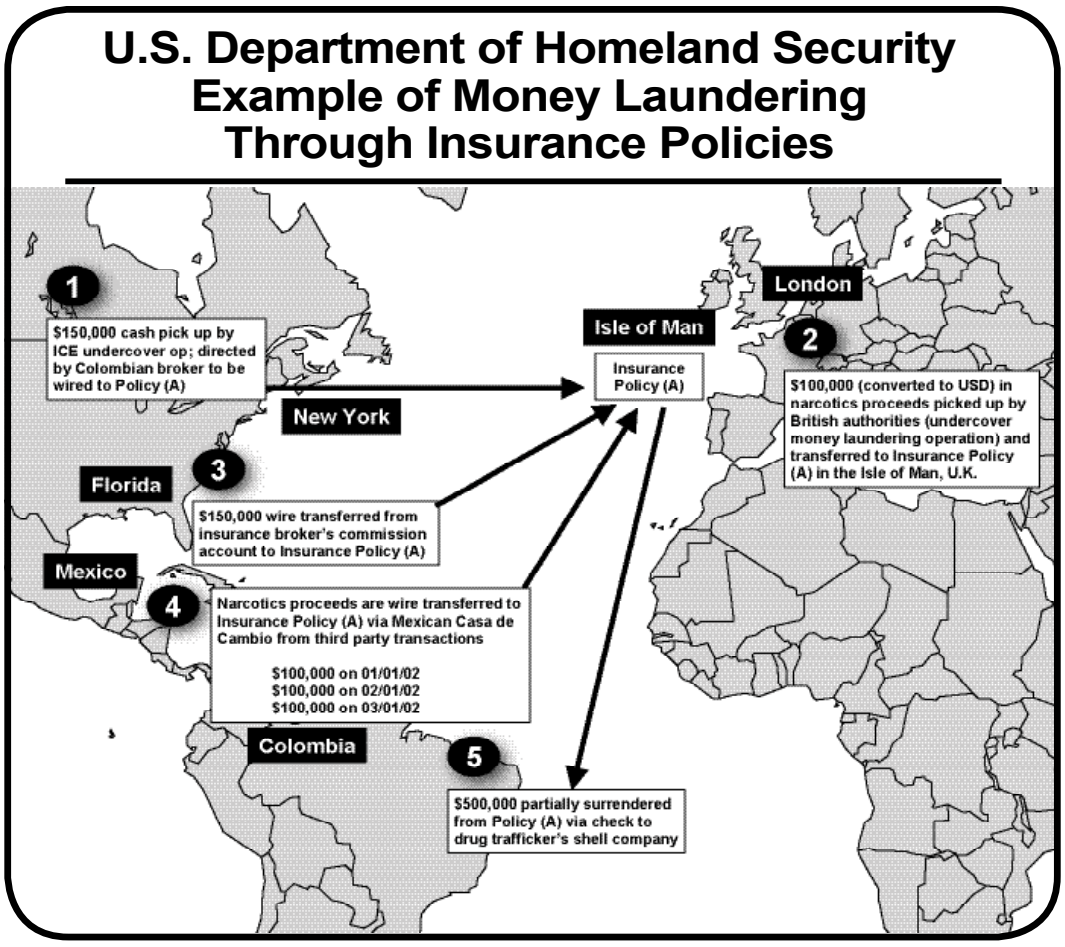
- Early redemption: One indicator of possible money laundering is when a potential policyholder is more interested in the cancellation terms of a policy than the benefits of the policy. The launderer buys a policy with illicit money and then tells the insurance company that he has changed his mind and does not need the policy. After paying a penalty, the launderer redeems the policy and receives a clean check from a respected insurer.

Real-Life Example

During a long-term drug trafficking investigation in the 1990s, agents from the U.S. Immigration and Customs Enforcement (ICE) in Miami learned that Colombian drug cartels were laundering large sums of money through the purchase of life insurance policies in Europe, the United States and offshore jurisdictions. Based on this information, ICE launched Operation Capstone in 2000. The probe found that Colombian cartels, using a small number of insurance brokers, were buying investment-grade life insurance policies with cartel associates as beneficiaries. The policies were purchased with drug proceeds sent to the insurance companies via wire transfers and checks by third parties around the globe. The investigation revealed that the cartels were then cashing out these policies after short periods of time, despite the financial penalties invoked for early liquidation. The cartel beneficiaries would then receive a check or wire transfer from the insurance company that appeared to be legitimate insurance/investment proceeds. The cartels could then use these "clean" funds. Agents determined that the cartels had used this scheme to purchase at least 250 life insurance policies and launder some $80 million in drug proceeds. In December 2002, ICE announced the seizure of nearly $30 million, the arrest of nine individuals, and charges against five additional individuals as a result of this joint probe by authorities in the United States, the Isle of Man, the United Kingdom, Colombia and Panama.

When a company assesses laundering and terrorist financing risks, it must consider whether it permits customers to:

- Use cash or cash equivalents to purchase insurance products.
- Purchase an insurance product with a single premium or lump-sum payment.
- Borrow money against an insurance product's value.



Source: United States Department of Homeland Security (http://www.dhs.gov/xlibrary/assets/Financial_Crimes_Press_Kit.doc)

SECURITIES BROKER-DEALERS

FATF has urged money laundering controls for the securities field since 1992, in conjunction with the Montreal-based International Organization of Securities Commissions (IOSCO), a global association of governmental bodies that regulate the securities and futures markets. Recognizing that other financial sectors have increased their defenses against money laundering, IOSCO said that it is important to "ensure that securities and futures markets do not become a comparatively more attractive alternative for money launderers." The difficulty in dealing with laundering in the securities field is that, usually, little currency is involved. It is an industry that runs by computer transfers and paper. Its use in the money laundering process is generally after launderers have disposed of their cash through other methods.

Aspects of the industry that increase its exposure to laundering are:

- Its international nature.
- The speed of the transactions.
- The ease of conversion of holdings to cash without significant loss of principal.
- The routine use of wire transfers from, to or through multiple jurisdictions.
- The competitive, commission-driven environment, which, like private banking, provides ample incentive to disregard the source of client funds.
- The practice of brokerage firms of maintaining securities accounts as nominees or trustees, thus permitting concealment of the identities of the true beneficiaries.

The illicit money laundered through the securities sector can be generated by illegal activities both from outside and from within the sector. For illegal funds originating outside the sector, securities transactions for the creation of legal entities may be used to conceal or obscure the source of these funds (layering). In the case of illegal activities within the securities market itself — for example embezzlement, insider trading, securities fraud, market manipulation — the transactions or manipulations generate illegal funds that must then be laundered. In both cases, the securities sector offers the launderer the potential for a double advantage: allowing him to launder illegal funds and to acquire additional profit from the related securities fraud.

Money laundering can occur in the securities industry in customer accounts that are used only to hold funds and not for trading. That allows launderers to avoid banking channels with more stringent money laundering controls. Other indications of money laundering are what are known as “wash trading” or offsetting transactions. These transactions involve the entry of matching buys and sells in particular securities, which creates the illusion of trading. Wash trading through multiple accounts generates offsetting profits and

losses and transfers of positions between accounts that do not appear to be commonly controlled.

Example

Josh opens a securities account at two brokerage firms with money that he made through drug trafficking. In one account, he takes a long position for a Eurodollar futures contract and, in the other account, he takes a short position for a Eurodollar futures contract. Whatever the market does, the losses and profits will offset each other, and he can request the proceeds of his activity in the form of a check from a reputable brokerage firm. This enables him to launder his money with minimal expenses, outside the costs of the transactions, without risking his principal, and, by using accounts at multiple firms, he decreases the likelihood of being detected.

Retail broker-dealers are the industry's frontline defense — and its most vulnerable access point. They are under constant management pressure to expand their client base and to manage more assets. The more assets in a client's account, the more commissions will be generated. A money launderer can potentially use this to his advantage by promising a large or steady commission stream.

Banks remain an important mechanism for the disposal of criminal proceeds. In this chapter, we described some special vulnerabilities for money laundering through banks and other depository institutions, such as electronic funds transfers, correspondent bank accounts, PTAs and private banking. The fact that other industries, such as car dealers, money remittance businesses, securities and insurance firms, have similar vulnerabilities to money laundering and criminal misuse provide ample evidence as to why they too have AML compliance program obligations.

NON-FINANCIAL BUSINESSES AND PROFESSIONS

CASINOS AND OTHER BUSINESSES ASSOCIATED WITH GAMBLING

Casinos are among the most proficient cash-generating businesses. High rollers, big profits, credit facilities and a variety of other factors combine to create a glittering amount of cash that flows from the house to the players and back. Where it is legally permitted, billions of dollars readily flow between the customer and casino.

Casinos and other businesses associated with gambling, such as bookmaking, lotteries and horse racing, continue to be associated with money laundering because they provide a ready made excuse for recently acquired wealth with no apparent legitimate source. The services offered by casinos will vary depending on the jurisdiction in which they are located and the measures taken in that jurisdiction to control money laundering.

Money laundering through casinos generally occurs in the placement stage, i.e., converting the funds to be laundered from cash to checks. A launderer can buy chips with cash generated from a crime and then request repayment by a check drawn on the casino's account. Often, rather than requesting repayment by check in the casino where the chips were purchased with cash, the gambler says that he will be traveling to another country in which the casino chain has an establishment, asks for his credit to be made available there and withdraws it in the form of a check in the other jurisdiction.

In its 1997-1998 typologies report, FATF says that gaming businesses and lotteries were being used increasingly by launderers. In its report, FATF gave examples of gambling transactions that enabled drug dealers to launder their money through casinos and other gambling establishments. One laundering technique connected with horse-racing and gaming is

when the person will actually gamble the money to be laundered, but in such a way as to be reasonably sure of ultimately recovering his stake in the form of checks issued by the gambling or betting agency and reflecting verifiable winnings from gaming. This method makes it more difficult to prove the money laundering because the person has actually received proceeds from gambling

Real-Life Example

On October 20, 1988, Waldemar Ratzlaf, a high-stakes gambler from Portland, Oregon, United States, lost $160,000 playing blackjack at the High Sierra casino in Reno, Nevada. He had been playing on a credit line extended by the casino which gave him one week to pay back the amount he lost. Seven days later he returned with $160,000 in cash to pay his debt to the casino. He asked the casino to refrain from reporting the cash transaction to the government, but was rebuffed. The casino vice-president told Ratzlaf that cashier's checks would be gladly accepted. To facilitate the process, the casino provided a limousine and driver to assist in the banking transactions. The next day, accompanied by a casino employee, Ratzlaf and his wife went to various banks in Nevada and neighboring California and purchased several cashier's checks, each for less than $10,000. They also asked several friends to purchase similar cashier's checks with cash they provided. By those means, the Ratzlafs were able to obtain enough individual cashier's checks with which to pay off their casino debt. In November 1990, the gambler and the casino employee who had accompanied him on their banking sojourn were indicted by a federal grand jury for, among other things, structuring cash transactions to prevent the filing of currency transaction reports.

DEALERS IN HIGH-VALUE ITEMS (PRECIOUS METALS, JEWELRY, ART, ETC.)

The European Directive on money laundering provides a common framework for including trade in gold, diamonds and other high-value items within anti-money laundering monitoring systems. Effective January 2006, the USA Patriot Act required certain dealers in covered and finished goods, including precious metals, stones and jewels, to establish an anti-money laundering program. However, in many other jurisdictions these industries are yet to be regulated for money laundering control purposes.

Gold is attractive to money launderers. As set forth by FATF in its 2002-2003 typology report, gold has high intrinsic value in a relatively compact form, which is easy to transport. It can be bought and sold easily and often with anonymity for currency in most areas of the world. It is more readily accepted than precious stones, especially since it can be melted down into many different forms. It holds its value regardless of the form it takes — whether as bullion or as a finished piece of jewelry — and is thus often sought after as a way of facilitating the transfer of wealth. For some societies, gold carries an important cultural or religious significance that adds to its demand.

FATF provided the following example:

Example

> An asset management company was responsible for managing the bank portfolios of two individuals active in gold purchases in Africa. The purchased African gold was sold to a gold working company in Country F, which, in turn, forwarded its payments to the sellers' accounts. Transfers were regularly made from these accounts to accounts in a European country. Wishing to verify the use of the funds, the asset management company asked its clients for a description of the channels used to pay for the gold in Africa. The information received permitted the company to identify an intermediary residing in Europe who was responsible for paying the suppliers in Country F. The

individual in question was described as being closely associated with a corrupt regime in Africa. Based on this information, the asset management company reported the case to the FIU and blocked the accounts. Information exchanged with foreign counterparts permitted this illegal trade to be linked to an ongoing foreign investigation, which targeted the same individual for arms trafficking.

In certain instances, some of the transactions in a particular scheme do not take place at all, but are represented with false invoicing. The paperwork is then used to justify transferring funds to pay for the shipments. The false invoicing scheme, whether over-billing or under-billing for the reputed goods or services provided, is a common money laundering technique.

The following transactions are also vulnerable, and require additional attention:

- **Payments or returns to persons other than the owner** — If one person delivers precious metal for refining and asserts ownership of the metal and authority to sell it, but directs payments to be made to another person, that transaction may be questionable. The "dealer in precious metal" is being used to transfer an asset not only from one form into another — e.g., unrefined gold to refined gold or money within the international finance system — but also from one person to another.

- **Precious metal pool accounts** — These accounts are maintained by a small number of large and sophisticated precious metal companies and have world-wide scope. They receive and hold precious metal credits for a customer, which can be drawn on by that customer. The customer can request the return of the precious metals, the sale and return of monetary proceeds, or the delivery of precious metal to another person. Thus, a refining customer in one country can deliver gold scrap for refining, establish a gold credit in the refiner's pool account system, and subsequently

have delivery made by the refiner to another person, based upon that credit.

Real-Life Case

On June 5, 2003, U.S. Immigration and Customs Enforcement (ICE) agents arrested 11 individuals at seven jewelry stores in Manhattan's diamond district on charges of participating in an international money laundering scheme. The agents had received information that Colombian drug cartels were laundering money through the purchase, smuggling and resale of diamonds and gold. The cartels were instructing their U.S. employees to buy precious stones in New York with drug proceeds and then to smuggle them to Colombia, where they were resold to refiners for "clean" pesos that the traffickers could use risk-free. Based on this information, ICE agents launched an investigation in 1999 into several New York jewelers alleged to be involved in the money laundering. According to the charges, the jewelers were approached by undercover agents posing as drug dealers. The agents told the jewelers they were looking to buy gold and diamonds with illicit funds so they could smuggle these precious metals to Colombia and then resell them to refiners for "clean" cash. According to the charges, the jewelers willingly accepted $1 million in drug funds from the undercover agents. The jewelers offered to smelt the gold into small objects, such as belt buckles, screws and wrenches, to facilitate smuggling the transfer into Colombia.

Illegal trade in diamonds has become an important factor in armed conflict in certain areas of the world, and terrorist groups may be using diamonds from these regions to finance their activities.

Individuals and entities in the diamond sector have also been involved in complex diamond-related money laundering cases. As with gold, the simplest typology involving diamonds consists of the direct purchase of the gems with ill-gotten money.

With regard to casinos and dealers in high-value items, FATF says that the more common types of laundering activity include retail foreign exchange transactions, the purchasing of gaming chips at casinos, forged or fraudulent invoicing, commingling of legitimate and illicit proceeds in the accounts of diamond trading companies, and, in particular, international funds transfers among these accounts. Some of the detected schemes were covers for laundering the proceeds of illicit diamond trafficking. In others, diamond trading was used as a method for laundering proceeds generated by other criminal activity.

The multi-million-dollar fine art industry can also serve as a convenient money laundering vehicle. Anonymous agents at art auction houses bid millions of dollars for priceless works. Payment is later wired to the auction house by the agents' principals from accounts in offshore havens. It is an ideal mechanism for the money launderer.

Real-Life Case

One famous case was Operation Dinero, a 1992 joint DEA and IRS operation. The agencies operated a fake bank in Anguilla targeting the financial networks of international drug traffickers. Several undercover companies were established by law enforcement in different jurisdictions as fronts designed to supply laundering services to the traffickers. Members of the Cali cartel engaged in transactions with the "bank" to sell three masterpieces by Picasso, Rubens and Reynolds that had a combined value of $15 million. The works were later seized by the U.S.

Art and antiques dealers and auctioneers should follow these tips to lessen their money laundering risks:

- Require all art vendors to provide names and addresses. Ask that they sign and date a form that states that the item was not stolen and that they are authorized to sell it.

- Verify the identities and addresses of new vendors and customers. Be suspicious of any item whose asking price is not commensurate with its market value.
- If there is reason to believe an item might be stolen, immediately contact the Art Loss Register (www.artloss.com), the world's largest private database of stolen art. The database contains more than 100,000 items reported by enforcement agencies, insurers and individuals as being stolen.
- Look critically when a customer asks to pay in cash. Avoid accepting cash payments unless there is a strong and reputable reason.
- Be aware of money laundering regulations.
- Appoint a senior staff member to whom employees can report suspicious activities.

TRAVEL AGENCIES

Travel agencies can also be used as a means for money launderers to mix illegal funds with clean money to make the illegal funds look legitimate, by providing a reason to purchase high-priced airline tickets, hotels and other vacation related expenses.

Real-Life Case

Operation Chimborazo, named for the famous Ecuadorean mountain, was a large multinational effort in the mid-1990s aimed at businesses suspected of laundering drug proceeds. The operation focused on the money laundering organization of Hugo Cuevas Gamboa, a reputed principal launderer for the Cali Cartel. In 1994, law enforcement teams cracked down on several businesses in Latin American countries, which included travel agencies. During a raid in Argentina, the authorities arrested the owners of a

travel agency that was part of an organization that laundered $50 million per week in drug proceeds from 22 countries.

Ways money laundering can occur in travel agencies include:

- Purchasing an expensive airline ticket for another person who then asks for a refund.
- Structuring wire transfers in small amounts to avoid recordkeeping requirements, especially when the wires are from foreign countries.

VEHICLE SELLERS

This industry includes sellers and brokers of new vehicles, such as automobiles, trucks, and motorcycles; new aircraft, including fixed-wing airplanes and helicopters; new boats and ships, and used vehicles.

Laundering risks and ways laundering can occur through vehicle sellers include:

- Structuring cash deposits below the reporting threshold, or purchasing vehicles with sequentially numbered checks or money orders.
- Trading in vehicles and conducting successive transactions of buying and selling new and used vehicles to produce complex layers of transactions.
- Accepting third-party payments, particularly from jurisdictions with ineffective money laundering controls.

Most money laundering cases dealing with vehicle dealers have one common element: the unreported use of currency to pay for the automobiles.

There have also been cases where authorities have charged that a car dealer laundered money by allowing a drug dealer to trade in his cars for cheaper models and to be paid in checks, not cash, for the

difference. In one such "down-trading" money laundering scheme, a drug dealer traded in his $37,000 Porsche for a $17,000 Ford Bronco and the car dealer allowed the down-trade, knowing that the customer was a drug dealer, in violation of the anti-money laundering law.

GATEKEEPERS: NOTARIES, ACCOUNTANTS, AUDITORS, LAWYERS

Countries around the world have been putting responsibilities on professionals, such as lawyers, accountants, company formation agents, auditors and other financial intermediaries, who have the ability to either block or facilitate the entry of illegitimate money into the financial system.

The responsibilities of such gatekeepers include requiring them to identify clients, to conduct due diligence on their clients, to maintain records about their clients and to report "suspicious" client activities. Some of these rules also prohibit gatekeepers from informing or "tipping off" clients who are the subject of the suspicious transaction reports. Violations may subject gatekeepers to prosecution, fines and even imprisonment.

In the European Union and several other countries, mandatory anti-money laundering duties already apply to "gatekeepers." The FATF 40 Recommendations also cover independent legal professionals (see next chapter about the FATF 40 Recommendations), including lawyers and legal professionals, and other "gatekeepers."

In its typology report of 2000-2001, FATF says that the following functions provided by lawyers, notaries, accountants and other professionals are the most useful to a potential money launderer:

- Creating corporate vehicles or other complex legal arrangements, such as trusts. Such arrangements may serve to confuse the links between the proceeds of a crime and the perpetrator.
- Buying or selling property. Property transfers serve as either the cover for transfers of illegal funds (layering stage) or the final investment of proceeds after they

pass through the initial laundering process (integration stage).

- Performing financial transactions. Sometimes these professionals may carry out various financial operations on behalf of the client (for example, issuing and cashing checks, making deposits, withdrawing funds from accounts, engaging in retail foreign exchange operations, buying and selling stock, and sending and receiving international funds transfers).

- Providing financial and tax advice. Criminals with large amounts of money to invest may pose as individuals hoping to minimize tax liabilities or seeking to place assets out of reach in order to avoid future liabilities.

- Providing introductions to financial institutions.

FATF cites the following example in its typologies report of how a lawyer may help set up a complex laundering scheme:

Example

This case involved 19 individuals in the medical service industry, along with a lawyer who was also an accountant. The prosecution alleged 123 violations involving conspiracy, false claims, wire fraud and money laundering and resulted in both primary defendants forfeiting property and millions of dollars and serving prison terms. The false claims involved fictitious patient claims and false service claims.

The two primary subjects employed the lawyer's services to set up related shell corporations to generate fictitious health care service records reflecting home therapy and nursing care. Health care providers, including therapists, registered nurses and physicians, operated the shell corporations. To keep the health care billing, tax return filings and bank account records synchronized, the two main subjects relied on the lawyer/accountant defendant.

> More than $4 million was laundered through bank accounts in cities in the north and southeast of the country and through suspected offshore accounts. Numerous accounts were created at four or five separate banks for the purpose of amassing and moving these funds. Cashier's checks were often purchased and even negotiated through the lawyer/accountant's trust account for concealment of property acquisition.

The issue of requiring attorneys to be gatekeepers in the anti-money laundering area has been controversial due to the fact that attorneys have a confidential relationship with their clients. Various alternatives have been discussed and debated, including:

- Deferring regulation until adequate education is conducted.
- Imposing internal controls and due diligence duties on lawyers with regard to non-privileged communications.
- Using a joint government-private sector body to regulate lawyers who engage in financial activities, requiring registration with and regulation by an agency such as the Financial Services Commission of the Channel Islands.
- Devising a new "hybrid" approach, such as through "guidance notes" or best practices standards from FATF.

Gatekeeper issues in the U.S. are focused on the scope of the requirements, particularly the definition of the financial transactions to which reporting requirements would apply. Many regulators within the U.S. want the scope to coincide with the European Union Directive, which requires EU members to ensure that the obligations are imposed on a wide range of professionals, including auditors, attorneys, tax advisers, real estate agents and notaries.

Even if the U.S. does not adopt gatekeeper standards like those of the EU and the UK, the extraterritorial reach of several existing initiatives already subject lawyers who conduct international transactions to various requirements.

INVESTMENT AND COMMODITY ADVISERS

Commodity futures and options accounts are vehicles that could be used to launder illicit funds. What are they?

- Commodities: Goods such as food, grains and metals that are usually traded in large amounts on a commodities exchange, usually through futures contracts.
- Commodity pools: Combines funds from various members and uses them to trade in futures or options contracts.
- Futures/futures contracts: Contracts to buy or sell a quantity of a commodity at a future date at a set price.
- Omnibus accounts: Accounts held by one futures commission merchant (FCM) for another. Transactions of multiple account holders are combined and their identities are unknown to the holding FCM.
- Options/options contracts: Contracts that create the right, but not the obligation, to buy or sell a set amount of something, such as a share or commodity, at a set price after a set expiration date.

Commodity trading advisers are persons who engage in the business of advising others, either directly or indirectly, as to the value or advisability of trading futures contracts or commodity options, or issue analyses or reports concerning trading futures or commodity options. Due to the fact that they direct such accounts, advisers are in a unique position to observe activity that may suggest money laundering. As such, they need to be aware of what types of activity may indicate potential laundering or terrorist financing and need to implement a compliance program to detect and deter such activity.

Others with similar responsibilities are:

- Commodity pool operator: Operator or solicitor of funds for a commodity pool, which combines funds from members and trades futures or options contracts.

- Commodity trading adviser: Direct or indirect adviser on buying and selling futures or commodity options.
- Futures commission merchant (FCM): A firm or person that solicits or accepts orders on futures contracts or commodity options and accepts funds for their execution.
- Introducing broker-dealers in commodities (IB-Cs): A firm or person that solicits and accepts commodity futures orders from customers but does not accept funds. There are two types of IB-Cs, guaranteed and independent.
- Guaranteed introducing broker: An introducing broker-dealer with an exclusive written agreement with a futures commission merchant that obligates the FCM to assume responsibility for the introducing broker's performance.
- Investment adviser: Persons who provide advice on securities and investments and manage client assets.

Here are several ways this industry is susceptible to money laundering:

- Withdrawal of assets through transfers to unrelated accounts or to high-risk countries.
- Frequent additions to or withdrawals from accounts.
- Checks drawn on, or wire transfers from, accounts of third parties with no relation to the client.
- Clients who request custodial arrangements that allow them to remain anonymous.
- Transfers of funds to the adviser for management followed by transfers to accounts at other institutions in a layering scheme.
- Investing illegal proceeds for a client.
- Movement of funds to disguise their origin.

The revelations of massive money laundering through Capcom, a Chicago-based commodity trading firm and subsidiary of London-based Capcom Financial Services Ltd., show how this industry can be used to launder money.

Real-Life Case

The shareholders of Capcom Futures Inc. of Chicago were the same wealthy Middle Eastern sheiks who invested in BCCI in the mid-1980s. The goals of Capcom were allegedly the misappropriation of BCCI assets for personal enrichment. This entailed laundering billions of dollars from the Middle East to the U.S. and siphoning assets from BCCI to create a safe haven outside the official BCCI financial empire. BCCI auditors said that when the commodities investments and huge trading losses were initially uncovered, they were duped into believing that BCCI had discontinued speculative trading. But BCCI surreptitiously continued its commodities trading activity by transferring funds to Capcom through a Panamanian shell corporation established for this purpose. Futures trading losses were disguised to deceive auditors. The commodities market was a natural fit for BCCI because of its minimal regulation and supervision, compared with the regulation of the banking and securities industries. Capcom took advantage of that regulatory atmosphere by engaging in substantial trading in speculative futures contracts. Profits were allocated to accounts of the firm's shareholders and the offsetting losses to BCCI accounts. The millions of dollars in trading commissions were allocated to accounts of Capcom's managers and officers. The Saudi investors were able to recoup their investment in BCCI by diverting funds through Capcom into their personal accounts. BCCI's losses from the Capcom operation exceeded $400 million, a leading cause of BCCI's insolvency. Investigations of Capcom uncovered widespread money laundering on behalf of BCCI involving

investments from Manuel Noriega, Lebanese drug proceeds, and West German Ponzi scheme proceeds. BCCI paid hush money of more than $30 million to one of its officials, fugitive Ali Akbar. The funds were deposited into a Capcom account and a paper loss on commodity trades was generated to offset the deposits.

TRUST AND COMPANY SERVICE PROVIDERS

Trust and company service providers (TCSP) include those persons and entities that, on a professional basis, participate in the creation, administration or management of corporate vehicles.

They refer to any person or business that provides any of the following services to third parties:

- Acting as a formation agent of legal persons.
- Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons.
- Providing a registered office, business address or correspondence for a company, a partnership or any other legal person or arrangement.
- Acting as (or arranging for another person to act as) a trustee of an express trust.
- Acting as (or arranging for another person to act as) a nominee shareholder for another person.

In an October 2006 report called “The Misuse of Corporate Vehicles, Including Trust and Company Service Providers,” FATF stated that, in many jurisdictions, the existence of TCSPs is not recognized. However, trust and company services may well be provided by lawyers and other professionals. For example, in most, if not all, jurisdictions, lawyers will be engaged in the formation of foreign companies for clients to hold assets (e.g., a yacht, a

residential or commercial property, etc) outside of that client's jurisdiction. FATF noted that some TCSPs are required to afford confidentiality privileges to a client, which can conflict with AML reporting requirements.

Although the vast majority of companies and trusts are used for legitimate purposes, legal entities or other types of legal relationships formed by these professionals remain common to money laundering schemes.

According to Transparency International, the reason to focus on service providers, rather than the company or trust, is that the latter are merely the tools through which the launderers operate. A company owned by criminals cannot protect itself, but service providers can, through diligence, reduce the risk of abusing the vehicles with which they have a relationship.

That is why it is important that countries regulate service providers. Regulations should stipulate how the service provider is to conduct its business, including how directors selected by the provider are to meet their obligations as trustees or trusteeships.

In its 2004 report, Transparency International said that the first jurisdiction to bring these activities under regulatory control was Gibraltar, which enacted legislation in 1989. Some other offshore jurisdictions have either introduced some form of regulatory control or will in the future. Regulations are not uniform; they range from a simple minimum capitalization requirement to full regulatory oversight. Often, the scope of the legislation is limited, excluding certain types of activities. Sometimes, the legislation bars regulators from gaining access to client files without client permission (or a court order), thereby making checks on the adequacy of the license-holder's Customer Due Diligence (CDD) provisions virtually impossible. Furthermore, while some jurisdictions include service providers within their anti-money laundering regulations — for example, by making compliance with the regulations a condition of licensing — many do not, leaving service providers free of any anti-money laundering duties beyond those imposed upon the general public. As a result of these differing standards, it is easy for a person seeking to use

a company or trust for criminal purposes to select a jurisdiction that either lacks requirements or has only inadequate ones, said Transparency International.

REAL ESTATE INDUSTRY

The real estate sector is frequently used in money laundering activities. The laundering cases that have involved the use of criminal proceeds in real estate transactions support the need for this sector to be under the anti-money laundering regulatory umbrella.

Investing illicit capital in real estate is a classic method of laundering dirty money, particularly in countries with political, economic and monetary stability. According to the March 2004 report, "Money Laundering in Canada: An Analysis of Royal Canadian Mounted Police (RCMP) Cases," nearly 56 percent of money laundering or proceeds of crime cases investigated by the RCMP involved real estate. The report said that deposit institutions and real estate firms constituted the "most significant sectors in laundering when measured by frequency of use, as well as the volume of criminal proceeds that enter the legitimate economy."

The report suggests this practice is likely because real property provides housing and shelter for criminals, and rural properties are ideal for growing and storing drugs. Also, proceeds of crimes can be readily funneled through the property using such transactions as deposits, down payments, mortgages, lawyers' trust accounts and even construction costs. The use of nominees, who hide the identity of the true beneficial owner, was found to exist in 46.3 percent of the cases, making it a popular laundering technique.

Laundering may be accomplished either by way of buying and selling real estate to hide the illicit source of funds (the layering phase), or by investment in, for example, tourist or holiday complexes that lend an appearance of legality (the integration phase).

In its 1997-1998 typology report, FATF cited a Scandinavian case involving a previously convicted drug trafficker who had made several investments in real estate and was planning to buy a hotel. An assessment of his financial situation did not reveal the source of

his income. Following his arrest and further investigations, he was sentenced for drug trafficking and money laundering to seven and a half years' imprisonment; about $4.4 million was confiscated.

Countless real estate and business deals are closed every day using escrow funds. Escrow accounts, generally maintained by real estate agents and brokers and other fiduciaries, are designed to hold funds entrusted to someone for protection and proper disbursement. They are attractive to money launderers because of the large number of diverse transactions that can pass through them in any deal. Escrow accounts are sometimes used as "middlemen" to complicate paper trails. Even a small U.S. title insurance agency will receive and disburse more than a million dollars a month from its escrow account. Nearly every real estate transaction requires the deposit of a large check from the mortgagee, as well as checks and cash required from the buyer at closing. A money laundering title insurance agent can make multiple deposits of cash on a given day at several banks in amounts under the currency reporting threshold, credited to different, non-existent closings. The deposits appear to be normal business activities, but they could very well represent the steady accumulation of funds for the purchase of real property by a person wishing to hide the origin of his funds. The monies ultimately may simply be paid outright by the escrow agent as cashier's checks obtained by him, as wire transfers, or as corporate or escrow checks to strawmen or shell corporations. Each closing entails numerous routine disbursements for things such as the payment of the proceeds to the seller, payoff of the mortgage, real estate commissions, taxes, satisfaction of liens and other payments.

To a bank and other observers, the disbursement of funds at a closing may appear to be all one legitimate set of transactions. Money laundering can be easily hidden because the size and volume of routine escrow account activity smoothes out the "spikes" (which describe sudden ups and downs in an account) or multiple deposits associated with money laundering. Escrow accounts can facilitate the movement of funds by cashier's checks, wire transfers or company checks to seemingly legitimate individuals or companies. Few financial institutions have policies or procedures concerning escrow accounts. Most banks treat them

like any other business account. Because of the large balances escrow accounts often maintain, banks are tempted to handle them gingerly. In some cases, they allow escrow account overdrafts and payments against uncollected funds with few penalties. Financial institutions are well advised to focus attention on them lest they be caught in the web of "willful blindness." Specific policies, procedures and controls to monitor escrow accounts are prudent things to implement.

In this industry we also see the "reverse flip." A money launderer might find a cooperative property seller who agrees to a reported purchase price well below the actual value of the property and then accepts the difference "under the table." This way, the launderer can purchase a $2 million dollar property for $1 million, secretly passing the balance to the cooperative seller. After holding the property for a time, the launderer sells it for its true value of $2 million.

In the "loan back" money laundering method, a criminal provides an associate with a specific amount of illegitimate money. The associate then provides a "loan or mortgage" back to the trafficker for the same amount with all the necessary "loan and/or mortgage" documentation. This creates an illusion that the trafficker's funds are legitimate. The scheme is reinforced through "legitimately" scheduled payments made on the loan by the traffickers.

MANIPULATION OF PRICES IN IMPORT AND EXPORT TRANSACTIONS

When men's briefs and women's underwear enter a country at prices of $739 per dozen, missile and rocket launchers export for only $52 each, and full toilets ship out for less than $2 each, one should notice the red flags. These manipulated trade prices represent money laundering, tax evasion and/or terrorist financing. John Zdanowicz, of Florida International University, and Simon Pak, at Pennsylvania State University, reported that in 2001 the U.S. lost about $53.1 billion in tax revenues caused by fraudulent transfer pricing schemes between U.S. companies and collusive foreign trading partners.

Using filtering software they created, professors Zdanowicz and Pak conducted seminal research into the manipulation of prices in international trade since 1991. Using data purchased from the U.S. Commerce Department, the software can detect abnormal pricing schemes involving every commodity that leaves or enters the U.S. They found that over-pricing or under-pricing imports and exports facilitates tax evasion, money laundering and terrorist financing. The professors concluded that the most popular fraudulent pricing scheme is to under-value exports instead of over-pricing imports. The government watches imports closely because of the revenues generated by import duties, but little attention is paid to the pricing of exports, leaving that avenue open to exploitation.

In a June 2006 report, called "Trade-Based Money Laundering," FATF defined trade-based money laundering as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports. Moreover, trade-based money laundering techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail.

Money launderers can move money out of one country by simply using their illicit funds to purchase high-valued products, and then exporting them at very low prices to a colluding foreign partner, who then sells them in the open market at their true value. To give the transactions an air of legitimacy, the partners may use a financial institution for trade financing, which often entails letters of credit and other documentation.

The 2006 FATF study concluded that trade-based money laundering represents an important channel of criminal activity and, given the growth of world trade, an increasingly important money laundering and terrorist financing vulnerability. Moreover, as the standards applied to other money laundering techniques become increasingly effective, the use of trade-based money laundering can be expected to become increasingly attractive.

BLACK MARKET PESO EXCHANGE

The Black Market Peso Exchange (BMPE) is a process by which money in the U.S. (could also be in another country, for example, countries in Europe) derived from illegal activity is purchased by Colombian (and other countries') "peso brokers" and deposited in U.S. bank accounts that the brokers have established. The brokers sell checks and wire transfers drawn on those accounts to legitimate businesses, which use them to purchase goods and services in the U.S.

Colombian importers created the BMPE in the 1950s as a mechanism for buying U.S. dollars on the black market to avoid domestic taxes and duties on the official purchase of U.S. dollars and on imported goods purchased with dollars. In the 1970s, Colombian drug cartels began using the BMPE to convert drug dollars earned in the U.S. to pesos in Colombia. Why? It reduced their risk of losing their money through seizures and they got their money faster, even though they paid a premium to the peso broker. Today, the BMPE facilitates the money laundering operations of the cartels and the illegal import of U.S. goods by Colombian firms.

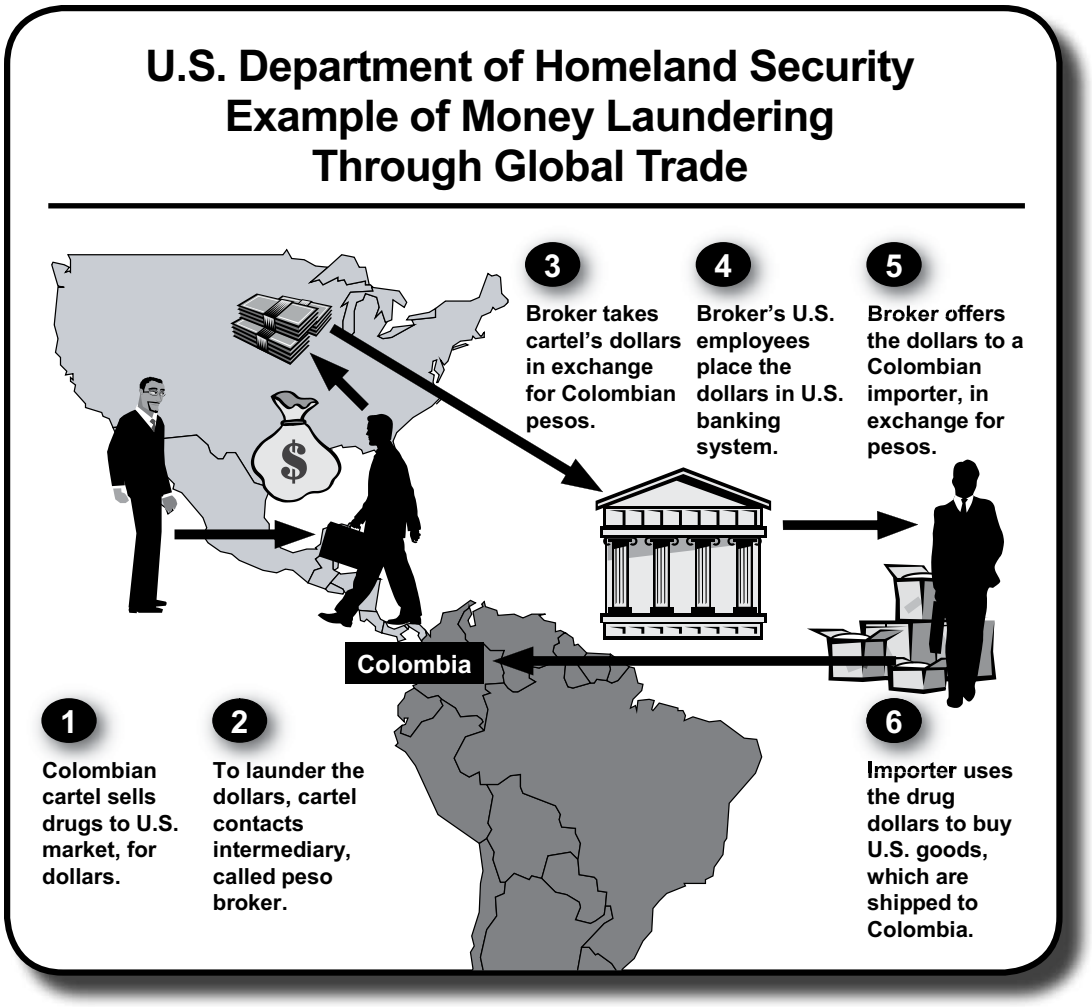
The Financial Crimes Enforcement Network (FinCEN) has issued advisories to U.S. financial institutions and corporations seeking help in combating this billion-dollar currency exchange and money laundering network.

MONEY LAUNDERERS CAN MOVE MONEY OUT OF ONE COUNTRY BY SIMPLY USING THEIR ILLICIT FUNDS TO PURCHASE HIGH-VALUED PRODUCTS, AND THEN EXPORTING THEM AT VERY LOW PRICES TO A COLLUDING FOREIGN PARTNER, WHO THEN SELLS THEM IN THE OPEN MARKET AT THEIR TRUE VALUE.

For financial institutions to detect and prevent laundering by peso brokers, they must be familiar with the common laundering methods used by the brokers. The most common scheme involves multiple checking accounts opened at U.S. banks by foreign nationals. Banks must also be aware of increases in the movement of dollars through correspondent accounts of foreign banks.

Real-Life Case

In 1997, U.S. Immigration and Customs Enforcement (ICE) agents launched an undercover investigation into a Colombian drug smuggling and money laundering organization. Over the next two years, undercover ICE agents posed as money launderers for this organization. They routinely picked up drug cash from organization employees in various U.S. cities and deposited it into undercover bank accounts. The Colombian organization then instructed the agents to wire the drug funds to specified accounts around the globe belonging to major U.S. companies. In one example, undercover agents were ordered by the Colombian organization to pick up a suitcase full of drug cash in New York. The next day, they were ordered to wire transfer $335,800 of the funds, in five separate payments, to an account belonging to a major U.S. company. ICE agents later determined that the wire transfers of drug proceeds to the U.S. company constituted partial payment for a helicopter the company was exporting to Colombia. The investigation further revealed that this U.S. company had received a total of 31 different wire transfers from individuals completely unrelated to the buyer as payment for the $1.5 million helicopter. In July 1999, ICE agents froze the funds they had wired to this company's account, as well as funds they wired to the accounts of other U.S. companies, on the grounds that the monies constituted drug proceeds. The investigation revealed that many of the U.S. companies had been paid in drug money for products that they were exporting to Colombia.



Source: United States Department of Homeland Security (http://www.dhs.gov/xlibrary/assets/Financial_Crimes_Press_Kit.doc).

MONEY LAUNDERING RISKS ASSOCIATED WITH NEW TECHNOLOGIES

Well-financed and technologically savvy criminals can move large amounts of funds easily and quickly from one country to another using electronic means.

ONLINE OR INTERNET BANKING

Many financial institutions offer customers access to their accounts via the Internet, with the same 24-hour services as those offered over the counter. These include consultation, transfers, wholesale cash management, automated clearinghouse services, funds transfers, bill presentment and payment, balance inquiries, loan applications and investment services. Although some online banking is offered by “pure” Internet banks (that is, only offering services through the Internet), institutions offering transactional services are, for the most part, established, traditional institutions that have moved into online banking as an additional customer service.

In its 1997-1998 typologies report, FATF said that Internet or telephone banking helps create distance between banker and client, and hence lessens or even eliminates the physical contact on which traditional client identification rested. While these services clearly have practical advantages for clients in terms of convenience, they make it more difficult to detect laundering activities because some of the traditional methods of supervision cannot be applied.

A significant money laundering risk for a financial institution offering online customer services is that there is greater difficulty in matching the customer with the provided identification documentation.

Other risks:

- The nature of online banking itself, with the elimination of face-to-face contact between customer and employee, necessarily makes it more difficult to know who is actually controlling the account.
- The ease of access through the Internet enables cross-border movements of funds from nearly every physical location.
- The rapidity of electronic transactions enables the execution of multiple, complex transactions within very short timeframes.

To combat cyberlaundering, FATF suggests that:

- Internet service providers establish log files with traffic data that produces Internet-protocol numbers of subscribers and telephone numbers used for server connections.
- Information collected through the servers be shared with law enforcement agencies.
- Information collected be maintained for up to a year.
- Internet service providers keep records, including identification information, on those who transit through their servers.

Just like "brick and mortar" banks, organizations that offer online banking should have procedures, whether they are driven by software, humans or a mix of the two, which verify the identity of anyone who seeks to do business with the institution. This can be difficult for online banks that often rely on customers to confirm who they are through passwords given the fact that passwords can be stolen or otherwise compromised.

Online banking will attract money launderers because of its potential to aid them in the three classic areas of money laundering:

- **Placement** — Launderers want to get their proceeds into legitimate repositories such as banks, securities or real estate, with as little trace of the source and beneficial ownership as possible. Often, cyberspace banks do not accept conventional deposits. However, cyberbanks could be organized to take custodial-like forms — holding, reconciling and transferring rights to assets held in different forms around the world. Money launderers can create their own systems shadowing traditional commercial banks in order to accept deposits, perhaps as warehouses for cash or other bulk commodities. Thus, cyberspace banks have the potential to offer highly secure, uncommonly private "placement" vehicles for money launderers.

- **Layering** — Electronic mail messages, aided by encryption and cyberspace banking transfers, enable launderers to transfer assets around the world many times a day.
- **Integration** — Once layered, cyberspace banking technologies may facilitate integration in two ways. If cyberbanking permits person-to-person cash-like transfers, with no actual cash involvement, existing currency reporting regulations do not apply. Using "super smart-card" technologies, money can be moved around the world through ATM transactions. These smart cards permit easy retrieval of the "account" balance by the use of an ATM card.

INTERNET CASINOS

According to FATF, Internet gambling might be an ideal web-based "service" to provide a cover for a money laundering scheme. There is evidence in some FATF jurisdictions that criminals are using Internet gambling to launder criminal proceeds. Despite attempts to deal with the potential problems of Internet gambling through regulation, requiring operating licenses, or banning such services outright, a number of concerns remain. For example, transactions are primarily performed through credit cards, and the offshore location of many Internet gambling sites makes locating and prosecuting relevant parties difficult, if not impossible.

According to the U.S. State Department's 2003 International Narcotics Control Strategy Report (INCSR), the Internet enables criminals to transfer funds instantaneously and enables poorly regulated offshore centers to increase their customer base. Virtual casinos are also profitable for governments, which sell licenses for the sites and may share in the operators' profits. Those governments exert inadequate controls, the report concludes, adding that the number of offshore financial centers with online gambling sites more than doubled between 2002 and 2003.

Real-Life Case

> In 2003, U.S. prosecutors in St. Louis, Missouri, alleged that, by processing payments for online gambling companies, PayPal, the big Internet payment service that facilitates the exchange of money via e-mail, violated the money laundering law prohibiting the international transmission of money derived from criminal activity. U.S. law makes it a crime to conduct a money transmitting business without a state license. This law was reinforced by the U.S.A. Patriot Act, which made it a crime for a licensed money transmitting company to send funds "known … to have been derived from a criminal offense or … intended to be used to promote or support unlawful activity." (Title 18, USC Sec. 1960.) PayPal paid $200,000 in penalties and forfeited its profits related to online gambling. PayPal stopped processing payments for online gambling companies in November 2002, a month after it was acquired by the online giant auctioneer, eBay. Hearings by the U.S. Senate Permanent Subcommittee on Investigations in 2001 disclosed that correspondent accounts of foreign banks at Bank of America and J.P. Morgan Chase had moved tens of millions of dollars in Internet gambling proceeds.

Some credit card issuers no longer allow use of its credit cards for online gambling, thus decreasing the money laundering opportunities through cyberspace.

How does an institution know whether a credit card is used for online gambling? The card relies on codes that indicate types of transactions. Many credit card statements list those category codes showing what customers spent on entertainment or travel, for example. The bank can thus block transactions coded for Internet gambling.

In a submission to FATF during its review of FATF's 40 Recommendations, the Interactive Gaming Council (IGC) pointed out that online gambling, with a combination of regulatory oversight and use of technology — while facing the same threats as real-

world gambling facilities — is in a good position to address these risks. “Online gambling does not lend itself to any form of cash movement because of the online nature of the business, specifically, there is no face-to-face contact in the business,” the IGC stated. Whatever exposure the interactive gaming industry has to money laundering can be mitigated through rigorous regulation, the organization added.

Nevertheless, online gambling provides an excellent method of money laundering because transactions are conducted principally through credit or debit cards. Site operators are typically unregulated offshore firms. This can affect a financial institution because the Internet gambling sites often have accounts in offshore banks that, in turn, use reputable domestic correspondent banks. Tracing the source and ownership of illegal money that moves through these accounts can be difficult for enforcement and regulatory agencies.

Real-Life Case

In a joint Russian-British operation in 2004, Russian police charged three men with extorting money from British online gambling companies by overwhelming their computers with huge amounts of e-mail and demanding money to relent. The gang members allegedly ran “a global protection racket netting hundreds of thousands of pounds from online sportsbooks,” according to Britain’s National Hi-Tech Crime Unit (NHTCU). According to press reports, police had followed a money trail from London, to the Caribbean, Latvia and then to Russia. “The recent arrests help to substantiate that there is a criminal motive behind this,” and not just individual hackers, said Ken Dunham, director of malicious code intelligence at Virginia-based iDefense Inc., a security consultant to government and business. According to the NHTCU, the gang had extorted UK companies “dozens of times” by bombarding their servers with messages from thousands of PCs at the same time. The so-called denial-of-service attacks overwhelmed

the companies' computers, forcing them to shut down and costing the companies "millions of pounds in lost business." Then the gang e-mailed demands for wired money – usually from €8,000 to €33,000 – in exchange for stopping the attacks.

PREPAID CARDS AND E-CASH

The following section contains excerpts from the 2006 New Payment Methods Report and 1998 Typologies Report from the Financial Action Task Force.

In October 2006, FATF published a report that examined the ways in which money can be laundered through the exploitation of new payment technologies (prepaid cards, Internet payment systems, mobile payments, and digital precious metals). The report found that, while there is a legitimate market demand for these payment methods, money laundering and terrorist financing vulnerabilities exist. Specifically, cross-border providers of new payment methods may pose more risk than providers operating just within a particular country. The report recommended continued vigilance to further assess the impact of evolving technologies on cross-border and domestic regulatory frameworks.

Pre-paid cards have the same characteristics that make cash attractive to criminals: they are portable, valuable, exchangeable and anonymous. The cards, many of which are branded by Visa or MasterCard, can be purchased and "loaded" with money by one person and used like regular debit cards by another person to make purchases or ATM withdrawals anywhere in the world.

Prepaid payment cards provide access to monetary funds that are paid in advance by the cardholder. While there are many different types of prepaid cards that are used in a variety of ways, the cards typically operate in the same way as a debit card and ultimately rely on access to an account. There may be an account for each card that is issued or, alternatively, there may be a pooled account that holds the funds prepaid for all cards issued. The cards may be issued by, and accounts may be held at, a depository institution or

a non-bank organization; pooled accounts would be normally held by the issuer at a bank.

The report identified these potential risk factors:

- Anonymous card holders;
- Anonymous funding;
- Anonymous access to funds;
- High value limits and no limits on the number of cards individuals can acquire;
- Global access to cash through ATMs;
- Offshore card issuers that may not observe laws in all jurisdictions; and
- Substitute for bulk-cash smuggling.

The prepaid cards' rapid proliferation and the absence of regulatory clarity in the U.S. prompted money services businesses to ask regulators to certify pre-paid card sellers, but regulations still do not exist. In Germany, however, adding value to a pre-paid card is considered the same as making a deposit. Therefore, pre-paid card issuers are considered credit institutions and must obtain full banking licenses and must follow the country's anti-money laundering regulations.

Electronic purses (also called e-purses or stored-value cards) are cards that electronically store value on integrated circuit chips. Unlike pre-paid credit cards with magnetic stripes that store account information, e-purses actually store funds on memory chips.

The use of these payment systems has declined considerably from 1996 to 2006, according to the 2006 FATF report. Only one, the German GeldKarte, operates in multiple jurisdictions – Germany and Luxembourg – with a limit of €200 ($254).

Measures that might limit the vulnerability to money laundering associated with these payment technologies are:

- Limiting the functions and capacity of smart cards (including the maximum value and turnover limits, as well as the number of smart cards per customer).
- Linking new payment technology to financial institutions and bank accounts.
- Requiring standard documentation and recordkeeping procedures for these systems to facilitate their examination.
- Allowing for the examination and seizure of relevant records by investigating authorities.
- Establishing international standards for these measures.

The terms "*pre-paid cards"* and "*stored-value cards"* are often used interchangeably. These cards can be broadly categorized into open (or open loop systems), semi-open, closed and semi-closed systems. As illustrated in Table 1, monetary value can be stored either in the central computer system or on the cards.

MONEY LAUNDERING RISKS OF STRUCTURES DESIGNED TO HIDE BENEFICIAL OWNERSHIP

SHELL COMPANIES

The use of shell and shelf companies to facilitate money laundering is a well-documented typology, according to FATF.

FATF offers the following definitions:

Shelf company: A corporation that has had no activity. It has been created and put on the "shelf." This corporation is then later usually

Table 1: Categories of stored value cards

Types	Description	Anonymous?	Reloadable?	Monetary value stored on card?	Examples
Open system cards	Typically 'branded' (e.g., by American Express), and connected to global debit and automated teller machine (ATM) networks, allow the cards to be used for multiple purposes and at multiple points of sale with participating merchants	Typically no -(similar in appearance to traditional debit cards, which are embossed with the cardholder's name and the expiry date)	Typically yes (e.g., via regular deposit arrangement, Internet and at participating merchant outlets)	Typically no — transactions are authorized online and in real time	Visa cash passport card(a), a reloadable pin-protected Visa-branded prepaid card, which allows cardholders to withdraw cash from Visa ATMs worldwide and use the cards at places where Visa debit cards are accepted
Semi-open system cards	Generally have the same features as open system cards but cannot be used to access cash at ATMs (also known as purchasing-only cards)	Typically no -(similar in appearance to traditional debit cards, which are embossed with the cardholder's name and the expiry date)	Typically yes	Typically yes — The value is stored on the cards, issuing merchants do not replace or refund stolen or misplaced cards	NETS CashCard(b)
Closed system cards	Limited to buying goods or services from the merchant issuing the card	Typically yes	Typically no, and sold at preset denominations, but some retail gift cards such as Starbucks gift cards are reloadable	Typically yes	Proprietary store / retail gift cards such as David Jones Gift Card(c)
Semi-closed system cards	Can be used at selected group of merchants or service providers	Typically yes	Typically no, and sold at preset denominations	Typically yes	FlyBuys(d) gift cardsd that can only be used at participating merchants

Notes: (a) http://www.cashpassportcard.com/ (b) http://www.nets.com.sg/consumers/netscashcard/index.php
(c) http://www.davidjones.com.au/gift_card.jsp (d) https://www.flybuys.com.au

sold to someone who would prefer to have a previously registered corporation than a new one.

Shell company/corporation: A company that at the time of incorporation has no significant assets or operations.

In October 2006, FATF issued a report called "The Misuse of Corporate Vehicles, Including Trust and Company Service Providers." In this report, FATF said that of particular concern was the ease with which corporate vehicles can be created and dissolved in some jurisdictions, which allows these vehicles to be used not only for legitimate purposes (such as business finance, mergers and acquisitions, or estate and tax planning), but also allows them to be misused by those involved in financial crime to conceal the sources of funds and their ownership of the corporate vehicles. Shell companies can be set up in onshore, as well as offshore locations, and their ownership structures can take several forms. Shares can be issued to a natural or legal person or in registered or bearer form. Some companies can be created for a single purpose or to hold a single asset. Others can be established as multipurpose entities.

When FATF reviewed the rules and practices that impair the effectiveness of money laundering prevention and detection systems, it found in particular that:

> *Shell corporations and nominees are widely used mechanisms to launder the proceeds from crime. The ability for competent authorities to obtain and share information regarding the identification of companies and their beneficial owner(s) is therefore essential for all the relevant authorities responsible for preventing and punishing money laundering.*

A 2001 report, "Money Laundering in Canada: An Analysis of RCMP Cases," offered four related reasons to establish or control a shell company for money laundering purposes:

1. Shell companies accomplish the objective of converting the cash proceeds of crime into alternative assets.

2. Through the use of shell companies, the launderer can create the perception that illicit funds have been generated from a legitimate source. Once a shell company is established, commercial accounts can be created at banks or other financial institutions. Especially attractive to money launderers are businesses that customarily handle a high volume of cash transactions, such as retail stores, restaurants, bars, video arcades, gas stations, food markets, etc. Illicit revenues can then be deposited into bank accounts as legitimate revenue, either alone or commingled with revenue legitimately produced from the business. Companies also offer criminals legitimate sources of employment in the community, which in turn helps cultivate an image of respectability.

Example

A small pizza business gets only 10 customers per day. Suddenly, according to its records, it is serving hundreds of clients per day. In reality, it still only receives 10 customers per day, so nothing had really changed.

Because the typical criminal does not like to spend money needlessly, in these types of front companies revenues have soared while expenses have remained the same. The pizzeria suddenly has hundreds of customers a day, but still books expenses (food, personnel, etc.) to serve only 10 clients.

Through this subterfuge, ill-gotten funds are funneled into a business, creating fake revenues consisting of illicit money. The illicit money is laundered by pretending it is revenue earned by these front companies.

Generally, front companies have some legitimate revenue, but their total revenue can come more from money generated by crime.

3. Once a shell company is established, a wide range of legitimate and/or bogus business transactions can be used to further the laundering process. These include lending money between criminally-controlled firms, paying out fictitious expenses or salaries, disguising the transfer of illicit funds under the guise of payment for goods or services, or purchasing real estate with the proceeds of crime or disguising payments for real estate as mortgages issued by a shell company. As a medium between criminal organizations and other laundering vehicles, shell companies are flexible and can be tailored to a launderer's specific needs. For example, criminal organizations laundering money through real estate can incorporate real estate agencies, mortgage-brokerage firms and development or construction companies to facilitate access to real property.

4. Shell companies can also be effective in concealing criminal ownership. Nominees can be used as owners, directors, officers or shareholders. Companies in Canada can also be incorporated as subsidiaries of corporations based in tax haven countries with strict secrecy and disclosure laws, thereby greatly inhibiting investigations into their ownership. Shell companies can also be used to hide criminal ownership in assets, by registering these assets, such as real estate, in the name of a company.

Shell companies are often legally incorporated and registered by the criminal organization, but have no legitimate business. Often purchased "off the shelf" from lawyers, accountants or secretarial companies, they are convenient vehicles to launder money. They conceal the identity of the beneficial owner of the funds; company records are often more difficult for law enforcement to access because they are offshore or are held by professionals who claim secrecy. In addition, few states in the United States ask for information about beneficial owners and even fewer attempt to verify any Information about beneficial owners.

Criminal enterprises also use real businesses to launder illicit money. These businesses differ from shell companies in that they operate legitimately, offering industrial, wholesale or retail goods or services.

While the vast majority of shell companies, or LLCs, are legitimate, once an illicit shell company is established, its primary objective is to claim the proceeds of crime as legitimate revenue and/or to commingle criminal proceeds with legitimate revenue.

The Canadian report mentions the following money laundering techniques used in conjunction with criminally controlled companies:

- **Using Nominees as Owners or Directors** — To distance a company from its criminal connections, nominees will be used as company owners, officers and directors. Nominees will often, but not necessarily, have no criminal record. Further, companies established by lawyers will often be registered in the lawyers' name.

- **Layering** — In some cases, a number of companies were established, many of them connected through a complex hierarchy of ownership. This helps to conceal criminal ownership and facilitates the transfer of illicit funds between companies, muddying any paper trail.

- **Loans** — Proceeds of crime can be laundered by lending money between criminally-controlled companies. In one case, a drug trafficker had $500,000 in a bank account in the name of a shell company. These funds were "lent" to restaurants in which the drug trafficker had invested. This seemingly legitimate use of the funds assisted in making it appear that the funds were being properly integrated into the economy. The $500,000 was repaid with interest to avoid suspicion.

- **Fictitious business expenses/False invoicing** — Once a criminal enterprise controls corporate entities in different jurisdictions, it can employ a laundering technique known as "double invoicing." An offshore

corporation orders goods from its subsidiary in another country, and the payment is sent in full to the bank account of the subsidiary. Both companies are owned by the criminal enterprise and the "payment" for goods is actually a repatriation of illicit money previously spirited out of the country. Moreover, if the subsidiary has charged a high price for the goods, the books of the parent company will show a low level of profit, which means that the parent company will pay less in taxes. It can also work the other way around. An offshore corporation buys goods from a parent company at price that is too high. The difference between the real price and the inflated price is then deposited in the subsidiary's account.

- **Sale of the business** — When the criminal sells the business, he has a legitimate source of capital. The added benefit of selling a business through which illicit money circulates is that it will ostensibly exhibit significant cash flow and, as such, will be an attractive investment and will realize a high selling price.

- **Buying a company already owned by the criminal enterprise** — An effective laundering technique is to "purchase" a company already owned by the criminal enterprise. This laundering method is most frequently used to repatriate illicit money that was previously secreted to foreign tax havens. Criminal proceeds from offshore are used to buy a company that is already owned by the criminal enterprise. In this way, the launderer successfully returns a large sum of money that had been secreted out of the country.

- **Paying out fictitious salaries** — In addition to claiming the proceeds of crime as legitimate business revenue, criminally-controlled companies also help make certain participants in a criminal conspiracy appear to be legitimate by providing them with salaries.

Sometimes, the stock of these shell corporations is issued in bearer shares, which means that whoever carries them is the

purported owner. Tax haven countries and their strict secrecy laws can further conceal the true ownership of shell corporations.

TRUSTS

Exact definitions of the term trust can be found in local laws and regulations. Although these definitions (and applicable regulations on trusts) vary across different jurisdictions, the term is generally defined in FATF's 2000-2001 typologies report as a legal relationship that is set up by a person (the "settlor") where assets have been placed under the control of another person (the "trustee") for the benefit of one or more persons (the beneficiaries) or for a specified purpose.

The significance of a trust account — whether onshore or offshore — in the context of money laundering cannot be understated: It can be used as part of the first step in converting illicit cash into less suspicious assets; it can help hide criminal ownership of funds or other assets; and it is often an essential link between different money laundering vehicles and techniques, such as real estate, shell and active companies, nominees and the deposit and transfer of criminal proceeds.

Given the private nature of trusts, in some jurisdictions they may be formed to take advantage of strict secrecy rules in order to conceal the identity of the true owner or beneficiary of the trust property. They are also used to hide assets from legitimate creditors, to protect property from seizure under judicial action, or to mask the various links in the money flows associated with money laundering or tax evasion schemes.

Payments to the beneficiaries of a trust can also be used in the money laundering process, because these payments do not have to be justified as compensation or as a transfer of assets for services rendered.

Lawyers often serve as trustees by holding money or assets "in trust" for clients. This enables lawyers to conduct transactions and to administer the affairs of a client. Sometimes, the illicit money is placed in a law firm's general trust account in a file set up in the

name of the client, a nominee, or a company controlled by the client. Also, trust accounts are used as part of the normal course of a lawyer's duties in collecting and disbursing payments for real property on behalf of clients.

Bearer Bonds and Securities

Bearer bonds and bearer stock certificates, or "bearer shares," are prime money laundering vehicles because they belong, on the surface, to the "bearer." When bearer securities are transferred, because there is no registry of owners, the transfer takes place by physically handing over the bonds or share certificates.

Bearer shares offer lots of opportunities to disguise their legitimate ownership. To prevent this from happening, FATF, in its 40 Recommendations, suggests that employees of financial institutions ask questions about the identity of beneficial owners before issuing, accepting or creating bearer shares and trusts. Financial institutions should also keep registries of this information and share it appropriately with law enforcement agencies.

Several FATF members do allow the issuance of bearer shares and maintain that they have legitimate functions in facilitating the buying and selling of such securities through book entry transfers. They also can be used, according to some sources, for concealing ownership for tax optimization purposes.

Bearer bonds and bearer stock certificates, or "bearer shares," are prime money laundering vehicles because they belong, on the surface, to the "bearer."

Bearer checks are unconditional orders (negotiable instruments) that, when presented to a financial institution, must be paid out to the holder of the instrument rather than to a payee specified on the order itself. Bearer checks are used in a number of countries. The financial institution is usually not obligated to verify the identity of the presenter of a bearer check according to international convention, unless the transaction exceeds a particular threshold. A non-bearer check may become a bearer instrument, payable to the individual who presents it, when the original payee has endorsed it.

TERRORIST FINANCING

After the terrorist attacks of September 11, 2001, the finance ministers of the Group of Seven (G-7) industrialized nations met on October 7, 2001, in Washington, D.C., and urged all nations to freeze the assets of known terrorists. Since then, many countries have committed themselves to helping disrupt terrorist assets by alerting financial institutions about persons and organizations that authorities determine are linked to terrorism. The G-7 nations marshaled FATF to hold an "extraordinary plenary session" on October 29, 2001, in Washington to address terrorist financing. As a result, FATF issued the first eight of its Special Recommendations. (See Chapter 3 for more detail.)

DIFFERENCES AND SIMILARITIES BETWEEN TERRORIST FINANCING AND MONEY LAUNDERING

Money laundering and terrorist financing are often mentioned in the same breath, without much consideration to the critically important differences between the two. Many of the controls that businesses should implement are meant to serve the dual purposes of combating both money laundering and terrorist financing. The terrorist financing indicators listed in the Financial Action Task Force's 2002 "Guidance for Financial Institutions on Detecting Terrorist Financing" were similar to those already established for combating money laundering.

But the two are separate crimes, and, while no one has been able to create a workable financial profile for operational terrorists, there are key distinctions that can help compliance officers understand the differences and can help distinguish suspicious terrorist financial activity from money laundering.

The most basic difference between terrorist financing and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. On the other hand, money

laundering always involves the proceeds of illegal activity. The purpose of laundering is to enable the money to be used legally.

In his presentation at Money Laundering Alert's 10th annual international conference in March 2005, James Richards, former anti-money laundering operations executive at Bank of America, and now with Wells Fargo, explained some of those differences.

The fact that terrorist money often has a legal source raises an important legal problem as far as applying anti-money laundering measures to terrorist financing. In several countries, terrorist financing may not yet fall under the definition of money laundering, or serve as a predicate offense for money laundering, and it may be impossible, therefore, to apply preventive and repressive measures to combat this problem.

From a technical perspective, the laundering methods used by terrorists and other criminal organizations are similar. Although it would seem logical that funding from legitimate sources does not need to be laundered, there is a need for the terrorist group to disguise the link between it and its legitimate funding sources. In doing so, the terrorists use methods similar to those of criminal organizations: cash smuggling, structuring, purchase of monetary instruments, wire transfers, and use of debit or credit cards. The hawala system also has played a role in moving terrorist related funds. In addition, money raised for terrorist groups is also used for mundane expenses like food and rent, and is not always strictly used for just the terrorist acts themselves.

DETECTING TERRORIST FINANCING

In its 2004 "Monograph on Terrorist Financing," the National Commission on Terrorist Attacks Upon the United States said that neither the September 11 hijackers nor their financial facilitators were experts in the use of the international financial system. The terrorists created a paper trail linking them to each other and their facilitators. Still, they were adept enough to blend into the vast international financial system without revealing themselves as criminals. The money laundering controls in place at the time were largely focused on drug trafficking and large-scale financial fraud

	Money Laundering	*Terrorist Financing*
Motivation	■ Profit	■ Ideological
Source of Funds	■ Internally from within criminal organizations	■ Internally from self-funding cells (increasingly centered on criminal activity) ■ Externally from benefactors and fundraisers
Conduits	■ Favors formal financial system	■ Favors cash couriers or informal financial systems such as hawala and currency exchange firms
Detection Focus	■ Suspicious transactions, such as deposits uncharacteristic of customer's wealth or the expected activity	■ Suspicious relationships, such as wire transfers between seemingly unrelated parties
Transaction Amounts	■ Large amounts often structured to avoid reporting requirements	■ Small amounts usually below reporting thresholds
Financial Activity	■ Complex web of transactions often involving shell or front companies, bearer shares, and offshore secrecy havens	■ No workable financial profile of operational terrorists exists, according to U.S. 9/11 Commission
Money Trail	■ Circular — money eventually ends up with person who generated it	■ Linear — money generated is used to propagate terrorist group and activities

Source: James R. Richards

and were not sufficiently focused on the transactions engaged in by the hijackers.

Real-Life Case

The September 11 hijackers used U.S. and foreign financial institutions to hold, move and retrieve their

money. They deposited money into U.S. accounts, primarily by wire transfers and deposits of cash or travelers checks brought from overseas. Several of them kept funds in foreign accounts, which they accessed in the United States through ATM and credit card transactions. The hijackers received funds from facilitators in Germany and the United Arab Emirates as they transited Pakistan before coming to the United States. The plot cost al Qaeda somewhere in the range of $400,000–$500,000, of which approximately $300,000 passed through the hijackers' bank accounts in the United States. While in the United States, the hijackers spent money primarily for flight training, travel and living expenses.

Through reconstruction of available financial information, the U.S. Internal Revenue Service and the U.S. Federal Bureau of Investigation established how the hijackers responsible for the Sept. 11 attacks received their money and how the money was moved into and out of their accounts.

The 19 hijackers opened 24 domestic bank accounts at four different banks. The following financial profiles were developed from the hijackers' domestic accounts:

Account Profiles:

- Accounts were opened with cash/cash equivalents in the average amount of $3,000 to $5,000.
- Identification used to open the accounts were visas issued through foreign governments.
- Accounts were opened within 30 days after entry into the U.S.
- All accounts were normal checking accounts with debit cards.
- Some of the accounts were joint accounts.

- Addresses used usually were not permanent addresses, but rather were mail boxes and were changed frequently.
- The hijackers often used the same address/telephone numbers on the accounts.
- No savings accounts or safe deposit boxes were opened.
- The hijackers opened their accounts at branches of large, well-known banks.
- Twelve hijackers opened accounts at the same bank.

Transaction profiles:

- Some accounts directly received/sent wire transfers of small amounts from/to foreign countries such as United Arab Emirates (UAE), Saudi Arabia and Germany.
- The hijackers made numerous attempts to withdraw cash in excess of the limit of the debit card.
- A high percentage of withdrawals were from debit cards.
- A low percentage of checks were written.
- Numerous balance inquiries were made.
- After a deposit was made, withdrawals occurred immediately.
- There was no discernible pattern with regard to the timing of deposits/disbursements.
- Overall transactions were below reporting requirements.
- Funding of the accounts was by cash and overseas wire transfers.

- ATM transactions occurred with more than one hijacker present (creating a series of transactions involving several hijackers at the same ATM).
- Debit cards were used by hijackers who did not own the accounts.

International activity:

- Three of the hijackers supplemented their financing by opening foreign checking accounts and credit card accounts at banks located in the UAE.
- While in the U.S., two of the hijackers had deposits made on their behalf by unknown individuals.
- Hijackers on all four flights purchased traveler's checks overseas and brought them into the U.S. Some of these traveler's checks were deposited into their U.S. checking accounts.
- Three of the hijackers continued to maintain bank accounts in Germany after moving to the U.S.
- Two of the hijackers had credit cards issued by German banks and maintained those cards after moving to the U.S.
- One of the hijackers received substantial funding through wire transfers into his German bank account in 1998 and 1999 from an individual.
- In 1999, this same hijacker opened an account in UAE, giving a power of attorney over the account to the same individual who had been wiring money to his German account.
- More than $100,000 was wired from the UAE account of the hijacker to the German account of the same hijacker in a 15–month period.

In an attempt clarify terrorist financing and offer recommendations to the global financial community, FATF has issued guidance to

identify techniques and mechanisms used in financing terrorism. The report, entitled "Guidance for Financial Institutions in Detecting Terrorist Financing," was published April 24, 2002, and describes the general characteristics of terrorist financing. Its objective is to help financial institutions determine whether a transaction merits additional scrutiny so that the institution is better able to identify, report (when appropriate) and ultimately avoid transactions involving the funds associated with terrorist activity. In the report, FATF suggests that financial institutions exercise "reasonable judgment" in evaluating potential suspicious activity. To avoid becoming conduits for terrorist financing, institutions are told they can look at, among other things, the following factors:

- Use of an account as a front for a person with suspected terrorist links.
- Appearance of an accountholder's name on a list of suspected terrorists.
- Frequent large cash deposits in accounts of non-profit organizations.
- High volume of transactions in the account.
- Lack of a clear relationship between the banking activity and the nature of the accountholder's business.

FATF suggests that, with these scenarios in mind, financial institutions should pay attention to some classic badges of money laundering, including dormant, low-sum accounts that suddenly receive wire transfer deposits followed by daily cash withdrawals that continue until the transferred sum is removed, and lack of cooperation by the client in providing required information.

HAWALA AND OTHER INFORMAL VALUE TRANSFER SYSTEMS

Hawala, hundi or so-called "underground banking" are alternative remittance systems or informal value transfer systems that are often associated with ethnic groups from Africa, Asia and the Middle East, and commonly involve the international transfer of

value outside the legitimate banking system. These informal value transfer systems are based on trust.

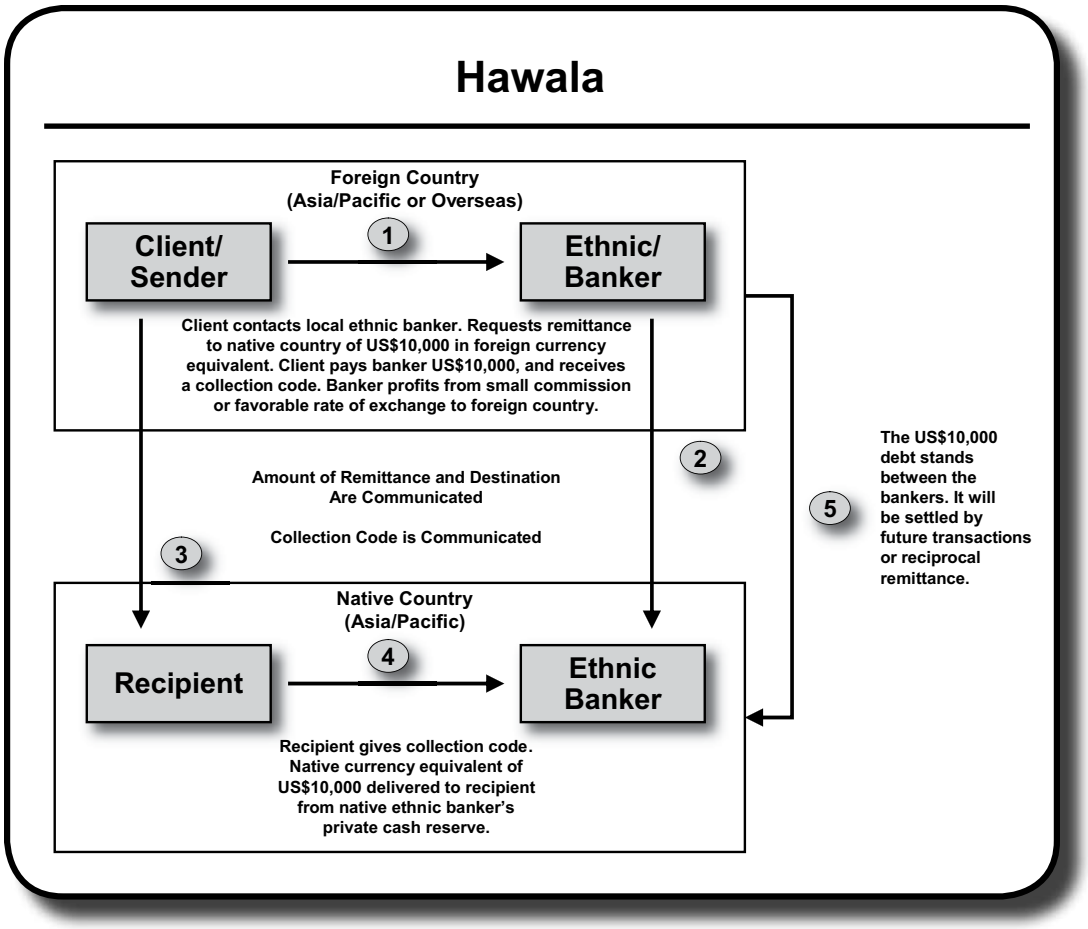
Hawala was created centuries ago in India and China, before Western financial systems were established, to facilitate the secure and convenient movement of funds. Merchant traders wishing to send funds to their homelands would deposit them with a hawala "banker," who normally owned a trading business. For a small fee, the banker would arrange for the funds to be made available for withdrawal from another "banker," normally also a trader, in another country. The two bankers would settle accounts through the normal process of trade.

Today, the process works much the same way, with people in various parts of the world using their accounts to move money internationally for third parties. In this way, deposits and withdrawals are made through hawala bankers rather than traditional financial institutions. The third parties are normally immigrants or visiting workers who send small sums to their homelands to avoid bank fees for wire transfers. As anti-money laundering measures have proliferated around the world, the use of hawala, which operates without governmental supervision, is believed to have become more appealing to money launderers and terrorists.

This method can be used to transfer both clean and dirty money. It is attractive for a launderer because it leaves little to no paper trail. The details of the customers who will receive the funds are faxed between the brokers.

Below you can find a chart from Interpol that shows the basic sequence of communication and payment in an alternative remittance:

Because hawala is a remittance system, it can be used at any phase of the money laundering cycle. It can provide an effective means of placement. When the hawalader receives cash, he can deposit the cash in bank accounts. He will justify these deposits to bank officials as the proceeds of legitimate business. He may also use some of the cash received to pay for his business expenses, reducing his need to deposit the cash into the bank account.



Source: Interpol

A component of many layering schemes is transferring money from one account to another, while trying not to leave a paper trail. A basic hawala transfer leaves little if any paper trail. Hawala transfers can be layered to make following the money even more difficult. This can be done by using hawala brokers in several countries, and by distributing the transfers over time.

Hawala techniques are used to transform money into almost any form, offering many possibilities for establishing an appearance of legitimacy in the integration phase of the money laundering cycle. The money can be reinvested in a legitimate (or legitimate appearing) business. The hawalader can very easily arrange for the transfer of money from the United States to Pakistan, and then back to the United States, apparently as part of an investment in a business there.

Hawalas are attractive to terrorist financiers because they, unlike formal financial institutions, are not subject to formal government oversight and do not keep detailed records in a standard form. Although some hawaladars do keep ledgers, their records are often written in idiosyncratic shorthand and are maintained only briefly.

Al Qaeda moved much of its money by hawala before September 11, 2001. Al Qaeda used about a dozen trusted hawaladers, who almost certainly knew of the source and purpose of the money. Al Qaeda also used both unwitting hawalas who probably strongly suspected that they were dealing with al Qaeda, but were nevertheless willing to engage in the transactions.

CHARITIES OR NON-PROFIT ORGANIZATIONS

Knowingly or not, charitable organizations have served as vehicles for raising and laundering funds destined for terrorism. As a result, some charities, particularly those with Muslim connections, have seen a large drop in donations or have become targets of what they claim are unfair investigations or accusations.

Charities or non-profit organizations have the following characteristics that are particularly vulnerable to misuse for terrorist financing:

- Enjoying the public trust.
- Having access to considerable sources of funds.
- Being cash-intensive.
- Frequently having a global presence, often in or next to those areas that are exposed to terrorist activity.
- Often being subject to little or no regulation and/or having few obstacles to their creation.

To help legitimate non-profit organizations avoid ties to terrorist-related entities and to help them regain public trust, FATF issued guidelines in 2002 on best practices for charities in combating the

abuse of non-profit organizations. The guidelines were related to FATF's Special Recommendations on Terrorist Financing. The practices cover all levels of a charity's operation, from administration and accounting to opening and maintaining bank accounts and foreign offices. FATF recommends that non-profit organizations:

- Maintain and be able to present full program budgets that account for all expenses.
- Conduct independent internal audits and external field audits, the latter to ensure funds are being used for intended purposes.

FATF recommends that charities use formal bank accounts to store and transfer funds so that they are subject to the bank's regulations and controls. The banks where the accounts are established, in turn, can treat non-profit organizations like other customers, apply their Know Your Customer rules and report suspicious activities.

SUMMARY

Money laundering occurs when funds from illegal activity are moved through the financial system in such a way as to make it appear that they came from legitimate sources.

Money laundering usually involves three stages: placement, layering and integration. In the placement stage, cash or cash equivalents are placed into the financial system. In the layering stage, the money is transferred or moved to other accounts through a series of financial transactions designed to obscure the origin of the money. Finally, in the integration stage, the funds are reintroduced into the economy so that they appear to have come from legitimate sources.

Money laundering can have several economic and social consequences, including increased crime and corruption, and the undermining of the legitimate private sector.

With regard to terrorist financing, the funds may be from illegitimate or legitimate sources. Even where they derive from legitimate sources, their movement may follow the money laundering pattern described above in order to disguise the origin of the funds.

As they have been historically, banks remain an important mechanism for the disposal of criminal proceeds. In this chapter, we described some special danger zones for money laundering through banks and other depository institutions, such as electronic funds transfers, correspondent bank accounts, PTAs and private banking. The several laundering cases that involved use of criminal

proceeds via non-bank transactions provide a strong argument for including other industries under the anti-money laundering umbrella, such as car dealers, money remittance businesses, and the securities and insurance industries.

New payment technologies, including prepaid cards, online banking and electronic cash, can widen the opportunities for laundering. Certain prepaid card and e-cash systems likewise present a risk in that no upper limit is set on transactions. In the absence of consistent standards and suitable monitoring by the supervisory authorities, these new payment technologies could well be vulnerable to money laundering operations.

Review Questions

- Name some indicators of money laundering in an insurance industry setting.
- What are the three stages of money laundering?
- What are the differences between money laundering and terrorist financing?
- How can money be laundered through real estate transactions?
- Why is private banking so vulnerable to money laundering?
- What are PTAs and what makes them vulnerable to money laundering?
- What structures are used by money launderers to hide beneficial ownership?