Risks and Methods of Money Laundering and Terrorist Financing

What is Money Laundering?
Simply put, money laundering is the process of making dirty money look clean. The goal of many crimes is to generate profit for the individual or group that carries out the criminal acts. Money laundering is the processing of those criminal proceeds to disguise their illegal source. It is of critical importance, since it enables the criminal to enjoy these profits without jeopardizing their source.

Crimes such as smuggling human beings, embezzlement, insurance fraud, bribery, drug trafficking and prostitution, can produce large profits, creating the incentive to “legitimize” the ill-gotten gains through money laundering.

When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without drawing attention to the underlying activity or persons involved. Criminals do this by disguising the sources, changing the form, or moving the money to a place where it is less likely to attract attention.

Money laundering can be defined generally as the process of concealing the existence, illegal source or application of income derived from criminal activity, and the subsequent disguising of the source of that income to make it appear legitimate. It is any attempt to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources.

Deception is the heart of money laundering: deceiving authorities by making assets appear to have been obtained through legal means with legally-earned income or to be owned by third parties who have no relationship to the true owner.

The Financial Action Task Force (FATF) — 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 — provided this “working definition” of money laundering:
• 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.

Among the FATF’s first accomplishments was to dispel the notion that money laundering is only about cash transactions. Through its several money laundering “typologies” exercises, the 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 of the three 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.

The FATF 40 Recommendations on Money Laundering 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 say that the intent and knowledge required to prove the offence of money laundering includes the concept that such mental state may be inferred from “objective factual circumstances.” In the U.S., the term “willful blindness” is a legal principle that operates in money laundering cases. Courts define it 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 the FATF expanded its mandate to cover the financing of terrorism. Whereas funds destined for money laundering are typically derived from criminal activities, such as drug trafficking and fraud, terrorist funding is different. Concealment is intended to hide the “purpose” for which these funds are used, rather than to conceal their origin, as with
criminal “profits.” Terrorist funds are sometimes not derived through illegal means. Generally, they are used for mundane expenses such as food and rent. Hence, funds are not only for the terrorist acts. Often terrorists use legal enterprises to conduct their business. While the fundraising process may often be within legal limits the use of charitable funds for terrorist purposes is something that is outside traditional money laundering scenarios. However, terrorists also covet secrecy of transactions and access to funds. Also, both terrorists and money launderers use the same methods to move their money, such as structuring payments to avoid reports 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 can generally distinguish three phases:

**Step One:** Placement — The physical disposal of cash derived from criminal activity. During this initial phase, the money launderer introduces his illegal proceeds into the financial system. Often, this is accomplished by placing it into circulation through financial institutions, casinos, shops, bureaux de change 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.

- Shipping cash across borders to deposit in foreign financial institutions, or to buy highvalue goods — such as artwork 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 obfuscate. The second stage involves converting the proceeds of crime into another form and creating complex layers of financial dealings to disguise the audit trail, source and ownership of funds. This phase can involve transactions such as:
- Wire transfers of deposited cash from one account to another
- Converting deposited cash into monetary instruments (e.g. traveler’s checks)
- Reselling high-value goods and monetary Instruments
- Investing in real estate and legitimate businesses.
• Use of shell banks, which are typically registered in offshore havens, and wire transfers.

**Step Three:** Integration — Supplying apparent legitimacy to illicit wealth by the re-entry into the economy of what appear to be normal business funds.

The third and final stage in the money laundering process, this stage entails placing laundered proceeds back into the economy to create the perception of legitimacy. By the integration stage, it is exceedingly difficult to distinguish legal and illegal wealth. The launderer might choose to invest the funds in real estate, luxury assets or business ventures.

**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 on Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT).”

Fears that anti-money laundering laws and regulations will undermine efforts to liberalize financial markets, or that opening up financial markets will promote money laundering, are unfounded. Money laundering threatens economic and financial systems in many countries, and the international financial community should strongly support anti-laundering efforts.

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, or 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 be smaller and therefore 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 will commit crime. Typically, havens for money laundering and terrorist financing have:
  
  - Limited number of predicate crimes for money laundering,
  - A restricted definition of institutions covered by money laundering laws and regulations,
  - Little enforcement of the laws, weak penalties, provisions that make it difficult to confiscate or freeze assets related to money laundering.

If money laundering is prevalent, there will also be more corruption, because the criminals will try to bribe government officials, lawyers and employees of financial or non-financial institutions so that they can continue to run their dirty business.

- **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, and 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, if not impossible, 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, which results 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. It 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. Furthermore, some financial crises of the 1990s — such as the fraud, money laundering scandal at 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.

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 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 the potential that adverse publicity regarding a bank’s business practices and associations, whether accurate or not, will cause a loss of public confidence in the integrity of the institution. Borrowers, depositors, and investors might stop doing business with the institution because of a money laundering scandal involving the institution. 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 by money launderers cannot be relied upon as a stable source of funding. Large amounts of laundered funds are often subject to unanticipated withdrawals from a financial institution through wire transfers, or government seizures, causing potential liquidity problems.

Operational risk is the potential for loss resulting from inadequate or failed internal processes, people and systems or external events. Such losses occur when institutions incur reduced, terminated or increased costs for inter-bank or correspondent banking services. Increased borrowing or funding costs can also be included in such losses.

Legal risk is the potential for lawsuits, adverse judgments, unenforceable contracts, fines and penalties generating losses, increased expenses for an institution, or even closure of such an institution. Money laundering involves criminals in almost every aspect of the money laundering process. As a consequence, legitimate customers may also be victims of a financial crime, lose money and sue the institution for reimbursement. There may be investigations, by banking or other law enforcement authorities resulting in increased costs, as well as fines and other penalties involved. 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. 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 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 criminal use of their members’ banking systems for the purpose of money laundering.

- **Loss of control of, or mistakes in, decisions regarding economic policy:** Because of 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 dollarized economies, as the tracking of monetary aggregates becomes more uncertain. And 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 interested in profit generation from their investments but rather in protecting their proceeds and hiding the dirty 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 proceeds, 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 shortterm interests of money launderers. When these industries no longer suit 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 if the untaxed proceeds of crime were legitimate.

A government deficit is at the center of economic difficulties in many countries, and correcting it is the primary focus of most economic stabilization programs. The IMF has been involved in efforts to improve the tax collection capabilities of its member countries. Although the small business sector is an important nexus of tax evasion, it also drives economic growth. It is therefore possible that many countries at a relatively early stage of economic development will be especially prone to tax evasion and the associated money laundering.

- **Risks to Privatization Efforts:** Money laundering threatens the efforts of many states 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 banks to hide their illicit proceeds and 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 from 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 will 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 government resources to rectify a problem that could be prevented with proper anti-money laundering controls. Other effects are specific counter-measures 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 a process vital to making crime worthwhile. It allows drug traffickers, smugglers and other criminals to expand their operations. This drives up the cost of government due to the need for increased law enforcement and health care expenditures (for example, for treatment of drug addicts) to combat the serious consequences that result.

The sheer magnitude of the economic power that accrues to criminals from money laundering has a corrupting effect on all elements of society. It could even lead to the virtual takeover of legitimate governments. Among its other negative socioeconomic effects, money laundering transfers economic power from the market, government and citizens to criminals.

**Methods of Money Laundering**

Money laundering is an evolving activity, and must be continuously monitored in all its various forms in order for measures taken in this effort to be timely and effective. Dirty money moves through offshore entities, wire transfers, trusts, hawala, securities dealers, car dealers, correspondent accounts, etc. Dirty money, like water, finds the route of least resistance. As many governments around the world have implemented anti-money laundering obligations for the banking sector, we see a significant shift in laundering activity from the traditional banking sector to the non-bank financial sector and to non-financial businesses and professions. Not only banks, but also non-bank
financial institutions and non-financial businesses have become attractive avenues for introducing illgotten gains into regular financial channels.

The 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 also to make certain that the FATF 40 Recommendations and Special Recommendations on Terrorist Financing remain effective and relevant. In this chapter we will refer often to these typologies, since they give good examples of how money can be laundered in different settings.

**Banks and Other Depository Institutions**

As they have been historically, banks remain an important mechanism for the disposal of criminal proceeds. Here are some special danger zones 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 electronic terminal, telephone, computer, automated teller machine (ATM) or magnetic tape. Typically, when someone wants to 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 go through the world’s wires each day.

Electronic fund 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 daily. Systems like Fedwire, SWIFT and CHIPS move many wires or transfer messages. Money launderers use electronic transfers of funds in the second phase of the laundering process, the layering cycle. Their goal is to move the funds around 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.
The money launderer will do the following to avoid detection, he will take basic precautions such as varying the amounts sent, keeping them relatively small if possible, and where possible he will use reputable organizations throughout the process. The rapid movement of funds between accounts in different jurisdictions increases the complexity of investigating and tracing the source of funds especially when non-customers transfer to equally unknown third parties.

The checks on electronic transfer of funds have been tightened. Many software providers have sophisticated algorithms to detect money laundering using electronic transfers of funds.

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

- 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 are received on behalf of a foreign client, with little or no explicit reason.

- Many small, incoming transfers of funds are received, or deposits are made using checks and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the customer’s business or history.

- Funds activity is unexplained, repetitive, or shows unusual patterns.

- Payments or receipts with no apparent links to legitimate contracts, goods, or services are received.

- Funds transfers are sent or received from the same person to or from different accounts.

**Correspondent Banking**
The Bank of New York 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,” found some of the great names in U.S. and foreign banking facilitate, through carelessness and lax procedures, the movement into the U.S. of diverse criminal proceeds.

In its Report on Money Laundering Typologies 2001-2002, the FATF said:

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, payablethrough 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 from another institution. This indirect relationship means the correspondent bank provides services for individuals or entities for which it has neither verified the identities nor obtained first-hand knowledge of the respondent’s customers.

2. Money laundering through correspondent accounts can pose a bigger threat to financial institutions than do customers who launder crime proceeds. That is because in a correspondent relationship astronomical amounts of money can come from many directions.
Additional risks incurred by the correspondent bank include:

- 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 is much more difficult.
- 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 farther removed from knowing the identities or business activity of these sub-respondents, or even the types of financial services provided.

The honeymoon is over for about 9,000 foreign financial institutions that have correspondent accounts in the United States. After decades of lucrative and virtually unexamined relationships, the USA Patriot Act of October 2001 had several provisions concerning the money laundering “gateway” that correspondent banking provides to foreign institutions. They include Section 312, which underscores the importance of money laundering control standards for correspondent accounts maintained for certain foreign banks. It says that 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. Other provisions include 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. The regulation under Section 319 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 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 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 what its regulatory history is.

**Example**
A lawsuit filed by a Hong Kong investor group in 2004 accuses 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 claims 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;
- Its chairman and managing director, Hakki Yaman Namli, was allegedly sought by Italian authorities in connection with laundering of $50 million.

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

**Payable-Through Accounts**
In some correspondent relationships, the foreign bank’s local customers are permitted to conduct their own transactions — including wire transfers, deposits withdrawals and maintain
checking accounts — through the foreign bank’s U.S. correspondent account. Those arrangements are called payablethrough accounts (PTAs).

These accounts often have a virtually unlimited number of subaccount 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 terms of the PTAs are specified in the agreement signed by the domestic and the foreign banks.

PTA accounts held in the names of foreign 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 foreign bank’s customer. But that is not always the case. Sometimes the sub-account holders are not identified to the domestic bank.

Elements of a PTA relationship that can threaten the domestic 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 domestic bank regards the foreign bank as its sole customer and fails to apply its Know Your Customer policies and procedures to the customers of the foreign bank,
- PTA arrangements in which sub-account holders have currency deposit and withdrawal privileges,
- PTAs used in conjunction with a subsidiary, representative or other domestic office of the foreign bank, which may enable the foreign 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, or PTA, at American Express Bank International in Miami. The Vanuatu bank offered its Central American customers virtually full banking services through its payable-through account at American Express Bank International. 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-acountholders 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 AEB. Over two years ending June 1993, as much as $200,000 in cash was received by Lombard’s Miami affiliate on 104 occasions. This small case with a limited outcome may serve as a clarion call to bankers about the dangers lurking in payable-throughs.

**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 risk 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 customer’s knowledge of concentration accounts or their ability to direct employees to conduct transactions through the accounts.
- Retaining appropriate transaction and customer identifying information.
- Frequent reconciling of the accounts by an individual who is independent from the transactions.
- Establishing timely discrepancy resolution process.
- Identifying recurring customer names.

**Private Banking**
This is not a side issue in the money laundering field. Private banking is an extremely lucrative, competitive and worldwide industry that has surfaced in almost every major money laundering case in recent years. In the early ‘90s 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 is at the bull’s eye of the tighter controls governments around the world urge. Competition brings increased pressures on the relationship managers and the marketing officers to obtain new clients, increase their assets under management, and 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.

**Example**

In the U.S. case of American Express Bank International, 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.”

These factors may contribute to private banking’s vulnerability to money laundering:

- Perceived high profitability and intense competition
- The high level of confidentiality associated with private banking
- The close relationships of trust developed between relationship managers and their clients.
- Commission-based compensation for relationship Managers

Often, private banking customers are “non-resident aliens.” Their assets often move overseas where they are held in the name of corporations frequently established by the domestic banks 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 conceal the identity of their beneficial owners. Many private banks establish PICs for their clients, often through an affiliated trust company in an offshore secrecy haven.

Another danger zone in private banking are the corrupt “Politically Exposed Persons,” who been warmly welcomed by many financial institutions.
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 to the U.S., maintained until 2001 private banking accounts for five years at Lehman Brothers in New York City containing some $20 million the DEA says he received in bribes from Mexican drug traffickers.

• The Riggs Bank case revealed a web of multihundred million dollar transactions that Riggs Bank had conducted over many years for dictators on two continents, including Augusto Pinochet of Chile and Teodoro Obiang Nguema of Equatorial Guinea. The accounts formed part of the embassy banking portfolio that was the bank’s specialty product for decades.

• Vladimiro Montesinos, the corrupt henchman 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 in which Montesinos had an interest.

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

• Pavel Lazarenko, the former prime minister of the Ukraine who is facing U.S. money laundering charges, had accounts in San Francisco at Bank of America, Commercial Bank, Pacific Bank, WestAmerica Bank, and securities firms, Fleet Boston Robertson & Stephens, Hambrecht & Quist and Merrill Lynch, where millions of dollars he allegedly extorted as head of state of the Ukraine were held.

• Colonel Victor Venero Garrido, a Peruvian army officer, whom the U.S. FBI described as “most trusted bag/straw man” of Vladimiro Montesinos, maintained accounts at Citibank in Miami and Northern Trust in California that 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, in the
mid-1990s maintained a private banking account at Texas Commerce Bank in Houston, where he deposited drug traffickers’ bribes of $9 million in currency over a 13-month period.

**Smurfing/Structuring**
Designing a transaction to evade triggering a reporting or recordkeeping requirement is called “structuring.” Structuring, or smurfing, 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, nicknamed “smurfs,” because they remind us of the mindless little blue creatures created by cartoonist Al Capp who run around doing whatever they were told to do. They go from bank to bank depositing cash and purchasing monetary instruments in amounts under the reporting threshold.

Smurfing can be done in many settings or industries, including the banking, money remittance and casino sectors.

**Examples**
- **A customer breaks a large transaction into two or more smaller ones.**
  Rick wants to conduct a transaction involving €18,000 in cash. However, knowing that it would exceed the cash threshold of more than €10,000 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 the threshold of €3,000 or more for recording of funds transfers would be met, 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 respectable travel agent and businessman — sophisticated, worldly, wise. He was nicknamed “Begin” because he looked so much like the Israeli prime minister. Hernan Botero ran a counting house and owned a fancy hotel and a percentage of several banks in Medellin, Colombia. Botero also held the
controlling interest in the Medellin soccer team, the city’s pride. He was a top sports promoter, a celebrity. Alberto Barrera owned a $400,000 house in South Florida. It had a swimming pool, expensive Oriental rugs and state-of-the-art electronics. His family lived there with him, enjoying the comfortable life of Colombian expatriates. From the house, Barrera directed a platoon of “smurfs” — persons who deposited cash at banks for him. He was Papa Smurf. All three men could be taken anywhere. They were comfortable at board meetings or at the country club. And all three were legendary money launderers for Colombia’s drug cartels: Experts in hiding, depositing, transferring and handling more than a billion dollars in profits from the sale of cocaine all across America. In a business rife with gangsters, gunmen and illiterate enforcers who kill and torture, money launderers are a breed apart. They are the drug barons’ representatives in polite society. To be successful, they must be intelligent and articulate, with a presence that is reassuring and sincere. They know how to procure a better table from the head waiter at an expensive restaurant. They use those same skills and personality traits in their business, to elicit what they want from bankers. Kattan laundered an estimated $500 million per year in cartel money, all of it cash. He kept his family in Colombia and lived quietly near downtown Miami, working out of four luxury condominiums. It was a convenient place to live. The city’s international banking center is housed in the flashy, glass-walled high-rises up the street. Couriers from a number of cities would visit Kattan 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. Kattan worked like a money changer. He bought dollars from drug dealers, paying them roughly 95% of the dollar value in pesos. The pesos were already in Colombian banks, and could be withdrawn by the drug suppliers there. Converting the dollars in Miami to pesos in Colombia was Kattan’s specialty. His favorite place for 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.) Kattan needed a way to invest his personal fortune. He found it among legitimate Colombian businessmen who wanted dollar loans to pay for goods in the United States. Kattan would lend them dollars from
his accounts in Miami to pay their U.S. suppliers. They would then repay the loans by depositing pesos in Kattan’s Colombian accounts, adding a money-changing percentage to the interest on the loan. Hernan Botero’s operation was smaller than Kattan’s. He laundered only about $100 million per year out of his home near Palm Beach. Colombian law enforcement knew Botero was the preferred launderer of Pablo Escobar, the alleged leader of the Medellin cartel. 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 in 1980. He was out of the country when the indictment was returned. It took five years to get him extradited to the U.S. for trial. 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 fronts. Occasionally, Botero showed up personally. He would use a hand truck to unload the trunk of his Mercedes Benz, rolling in the duffel bags stuffed with cash. Botero was convicted of moving $57 million through that one bank. 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. The last step was moving the money into dollar bank accounts in Bogota. Because Colombian law limits peso-to-dollar transfers up to $20,000, there were many of them. The entire system was labor-intensive. Officials theorize that Botero and his smurfs worked for Escobar instead of earning a percentage, as did Kattan and other independents. By the early 1980s, after the federal Operation Greenback had stung Botero, Kattan and others, Florida banks became nervous and knowledgeable about giant cash deposits. They were more religious about filing CTRs. Finding bankers to bribe became more difficult. The risk was too great. In 1983, Operation Greenback rolled up Barrera’s operation, arresting 16 smurfs. As luck would have it, Barrera was in Colombia that day. Kattan and Botero are serving 30-year sentences in federal prison.

Here is how foreign “money brokers” conduct what is called “bank account smurfing”:

- An “account smurfer,” who is acting for a foreign money broker, opens numerous checking accounts in Country A
using real and fictitious names. Sometimes the account smurbers use identification documents of dead persons supplied by the money brokers.

- With funds supplied by the money brokers, the account smurfer opens the accounts with inconspicuous amounts, usually in the low four-figures.
- To allay bank suspicions, the money brokers sometimes pay living expenses of their account smurbers into the accounts to give the accounts an air of legitimacy.
- Once the accounts are opened, the account smurfer 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.
- An account smurfer 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, the Paris-based Financial Action Task Force 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.

Cuckoo is the name of 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 smurfing and cuckoo smurfing is that in the latter the third
parties that hold the bank accounts used are not aware of the fact that dirty money is being deposited into their accounts.

Here is how it works: An alternative remittance system operator in South Asia or the Middle East buys private or commercial transfers to Europe. According to the FATF, some bank managers in Pakistan sell to remittance system operators genuine personal electronic transfers to be performed on behalf of legitimate customers. A controller – the person who oversees the entire laundering operation for the criminals – in Iran buys dirty cash from criminals and gives it to a collector in the U.K. along with the account details of a legitimate bank customer, who is expecting genuine transfers, perhaps from a family member overseas. The collector then deposits the criminal cash into the legitimate customer’s account in small amounts at multiple branches of the bank. In this way, the technique is similar to smurfing. The collector sends the deposit slips to the controller to prove that the cash was paid to the customer expecting transfers. The operator of the bank account is then contacted to be told that the transfer is complete. Individual deposits are increasingly reduced in size to avoid detection by the bank teller. The technique relies on the fact that
banks do not routinely seek the identification of people depositing money into accounts, and that CCTV (closed-circuit television) footage is routinely recorded over. It is the bank customer’s legitimacy that makes this type of laundering difficult to detect.

The FATF recommends that banks have controls in place to identify depositors who pay cash into third-party accounts. Also, banks should be on the lookout for unusual cash deposits that are structured or made in branches other than where the customer’s account is held.

According to the 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 should be subject to suspicious activity reporting;
- Law enforcement will need information on the depositor, so banks should seek to identify cash deposits made by third parties and retain surveillance footage.

**Bank Complicity**

A criminally co-opted bank employee might facilitate money laundering. Institutions and businesses have learned at great pain in recent years 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, or potentially the “enemy within,” is as crucial to a company’s security as knowing customers and other “outsiders.” (See also the section on AML Compliance Programs)

While regarding all prospective employees as potential “enemies” or implementing processes to uncover the “enemy
within” might seem unduly paranoid, the fact is that one individual or small group can wreak substantial damage if not identified. The Bank of New York case is a good example.

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

Background screening of prospective and current employees, especially for criminal history, is essential to keeping unwanted employees out and identifying those to be removed.

**Credit Unions or Building Societies**
The United Kingdom’s Joint Money Laundering Steering Group (JMLSG) stated in a November 2006 guidance that though credit unions pose low money laundering risk, they still have similar vulnerabilities to money laundering and terrorist financing schemes as their banking brethren. On the plus side, their relatively small size, compared to banks and other financial institutions, makes it harder for scammers to cleanse illicit cash because suspicious activity can be more quickly reported, the JMLSG report found. And, it makes it easier for credit union employees to comply with UK regulations such as: customer identification for transactions €15,000 or over [approximately U.S.$20,000] and verifying identity at account opening.

The JMLSG, a group of the leading UK financial services trade associations, which has been producing money laundering control guidance since 1990, said that there are two main kinds of credit unions: the first type only offers basic savings and loan products – referred to as Version 1 credit unions – and the second offers a broader range of financial services, known as Version 2.

Not surprisingly, the report noted, Version 2 operations pose a higher risk for money laundering since they tend to contain a larger clientele and offer potential criminals a larger range of possible ways to conceal their illicit funds. Overall, though, both types contain “high levels of cash transactions,” which increases the risk of money laundering or terrorist financing.
The group concluded that other high-risk transactions are: 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 draw less attention.

To combat these risky operations, the group suggested that credit unions create formal written policies that outline efficient ways to lower money laundering risk.

These policies should contain, at the minimum:
- Measures to identify risks specific to the credit union; paying close attention to clientele, products, and the institution’s location.
- Outlines for managing and controlling the assessed risks.
- Methods for monitoring and improving internal operations.
- Documentation of steps taken to prevent risk and the reasons behind those decisions.
- Instructions on record-keeping procedures.

Besides the written policy, the group also said that employees need to be trained on how to spot and deal with potential laundering, learn enhanced due diligence procedures and know the responsibilities of the money laundering officer.

**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;
• And 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 dirty funds that he somehow 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 is layering. Josh then uses dirty money he already placed in a bank account to pay a credit card bill for a new kitchen that he bought. So, now he has integrated his illicit funds into the financial system.

Once a bank receives a check payment for a credit card account, it is difficult to find out how the funds were put into the system and what their source was. If a money launderer is able to deposit funds into another institution, he could easily obtain a credit card. A money launderer could also 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. Here is one of them: “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 on-line 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 ethnic groups, since they charge lower commission rates than banks for transferring money abroad and have more flexible opening hours. Funds are often transferred to the least advanced regions of the world, where no proper banking services exist.

In its report on money laundering typologies of 1996-1997, the FATF said they operate in a variety of ways, but most commonly a business 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 (like Western Union and Money Gram);
- Money transfer systems connected with clandestine banks (underground banking); (We will discuss these 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 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 funds transfer networks serving ethnic groups; they may also
apply to official networks like those of the postal service. The
1997-1998 FATF report on money laundering typologies says
that the authorities of a Scandinavian country have noticed a
steep increase in international money orders to the countries of
the former Yugoslavia. In a FATF member country, the mails are
used to send packages containing large cash sums and even
drugs anonymously.

However, this industry is fighting an old myth, namely that it
consists of businesses that are uniformly “high risk” for money
laundering. This is not true. The biggest misconception about
this industry and especially is that they are lightly regulated; in
fact, they are usually just as regulated as banks that offer
equivalent services and often have extremely tight compliance
programs in place. 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. 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,” about which there is 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 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
when exchange offices became regulated, and it became subject
to obligations to prevent money laundering. The Counter often
had a surplus of bank notes with a high denomination, and 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. 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 and dealing in soft drugs, and because of this he transferred ownership of The Counter to a new owner with no police record (Andre). Andre registers The Counter to the Central Bank as an exchange office and is accepted on a temporary basis. The financial intelligence unit consults various police files and establishes that the police have been observing this exchange office for some time. The suspect transactions are passed on to the crime squad in the town where The Counter has its office, and it starts an investigation. A few months later, the crime squad arrests Andre, house searches are made, expensive objects and an amount equivalent to more than US$ 250,000 in cash are seized. The records of The Counter show that many transactions were kept out of 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, which used the exchange office to launder their proceeds, and this formed a substantial part of the turnover of the business.

The lesson of this case is 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 with them.

With the introduction of the Euro, and the elimination of 11 national currencies in the European Union — such as the deutschmark, Dutch guilder, and French franc — the role of money exchange houses (or bureaux de change, casas de cambio, as they are sometime called) in euro zone countries has diminished with regard to laundering.

**Insurance Companies**
In its 2002-2003 typologies report, FATF experts submitted case examples that show the vulnerabilities of the insurance sector to money laundering. The primary emphasis in the examples is on
the investment aspect of life insurance policies. 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. Another similarity between is that insurance brokers may often be the weak link in implementing anti-laundering measures. We will discuss the securities industry in the next section.

Most significant laundering and terrorist financing risks in the insurance industry are found in life insurance and annuities products. 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.

By comparison 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.

But relatively complex cases involving single premium contracts have recently been discovered which reveal less rapid procedures and less liquid transactions, allowing longer-term laundering that may offer criminals a degree of safety.

Vulnerabilities in the insurance sector include:

- Lack of oversight/controls on intermediaries: Insurance brokers have a great deal of control and freedom regarding policies. They often maintain pre-signed payment instructions for policy withdrawals to enable clients to make such withdrawals with a telephone call. Brokers sometimes pay insurance premiums from their own accounts; presumably they are reimbursed by the client in cash.
• Lack of training: Insurance brokers often have no or little training in anti-money laundering issues and can be used to place cash funds into various financial institutions. Some insurance companies fail to identify indicators of money laundering, such as payments for insurance products by unrelated third parties or use of consecutively numbered checks or money orders.

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

• Lack of knowledge: In addition to a lack of knowledge of the client and the source of his or her funds, insurers often have little knowledge of the complex pyramid of sub-brokers employed by their agents.

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, moving funds into and out of the policy for the cost of early withdrawal penalties. When such funds are reimbursed by the insurance company (by check, for example), the potential launderer has successfully obscured the link between the funds and the crime that generated them.

• 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.

• Early redemption: One indicator of possible money laundering is when a potential policyholder is more interested in cancellation terms of a policy than the benefits of the policy. The launderer buys a policy with dirty money and then tells the insurance company that he has changed his mind and does not need the policy after all. 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 use these “clean” funds virtually without question. Agents determined 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.
Securities Broker-Dealers
The FATF has urged money laundering controls for the securities field since 1992, most notably in a November 1992 report prepared in cooperation 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 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 blips and paper. Its use in money laundering comes after launderers have disposed of their cash through other means.
Aspects of the industry that increase its exposure to laundering are:

- Its international nature
- Fast-paced transactions, often at the click of a mouse
- The easy 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 maintaining securities accounts as nominees or trustees, thus permitting concealment of the identities of the true beneficiaries

The dirty 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 or 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 laundering controls. Other indications of money laundering are what are known as “wash trading” or offsetting transactions. Those involve the entry of matching buys and sells in particular securities, which creates the illusion of trading. Wash trading through multiple accounts generating offsetting profits and losses and transfers of positions between accounts that do not appear to be commonly controlled are other indicators of money laundering.

**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 where he makes the profit, he receives a check from a reputable brokerage firm.

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 bases and gather assets. The more assets in a client’s account the richer it is as a source of commissions, which is how brokers are compensated. The industry is a magnet for aggressive overachievers. The skilled launderer ideally would like to pluck an inexperienced registered rep and orchestrate a series of transactions by promising a commission stream. But brokerage managements and compliance officers watch inexperienced reps carefully. Senior brokers, on the other hand, are thought to be more secure financially and less likely to accept questionable clients. But launderers will do business where profit potential exists.

Consider this recent case quoted from a 2003 article from Money Laundering Alert written by Walter MacCarron, a broker with Sterling Financial Investment Group in California. It involves the Northern California office of a regional brokerage.

**Real-Life Example**

A wealthy individual who managed a large portfolio of his and some associates’ money obtained a referral to the brokerage. He flaunted his sophistication and demanded a seasoned broker. With no adverse reports on terrorist or narcotics ties from the U.S. Treasury’s Office of Foreign Assets Control or other outside sources, a broker with 25 years experience opened accounts for him to trade low-priced technology stocks. Management ignored red flags. This individual resided in Vancouver, British Columbia, yet wanted transactions cleared through a bank in the Cayman Islands. Those elements would normally prompt a demand to leave large deposits on account in case problems arose in clearing trades. Clearing, or settling, a transaction means either paying for the shares purchased or delivering the shares sold. That usually happens on the third business day after the transaction. Some investors want their transactions handled by their bank on a DVP basis, meaning the bank pays for a purchase when the shares are delivered to it. That’s what the brokerage agreed to, which was a stretch of good judgment, considering
the Caymans’ reputation for shielding the sources of bank accounts.

The second leg of the launderer’s scheme was now complete. A series of accounts was opened. Management’s attention shifted to seeking new clients and new business. It was time to set up the hit. The initial transaction was a purchase of 400,000 shares of an over-the-counter tech stock for $0.50 per share. The shares were delivered to the Cayman bank and paid for. All went well. The commission was higher than normal. The seeds of deception were sown. A week later another unsolicited order was given to the broker for 800,000 more shares of the same stock; the price was still $0.50. The stock in question had a small “float,” meaning the number of shares available for trading was relatively low and an order of this magnitude would have moved the share price. Indeed, the stock soared, closing that day at $0.92. The broker was elated, and the client seemed happy. On settlement date, however, the customer did not pay for the shares. He offered a lame excuse for the delay but reassured the broker. Meanwhile the share price began to weaken. When the extensions allowed for late payment were used up – a total of seven days -- the share price had fallen to $0.50. Compliance officers speculated that the 400,000 shares acquired a week earlier were probably sold at the same time the brokerage bought the 800,000 shares. That purchase ran up the share price and enabled the money launderer to make approximately $160,000 on money that was already illicit. For the brokerage, however, Federal Reserve margin rules require the shares to be liquidated back into the marketplace when the extensions are used up. With such a thinly traded stock, unloading 800,000 shares would drive the price down, and the brokerage estimated its loss at $350,000. In such cases a brokerage has few options. It can look to the individual broker for restitution. Generally, managements seek to avoid embarrassment and regulatory scrutiny, and seek to bury the matter under the rug. This time, the firm did fight back by calling in the FBI to see what could be recovered. But such “pump and dump” schemes – which launderers refer to as “cold showers,” meaning they get in and out quickly -- have become common in the securities industry, imposing costs and diverting resources far better used elsewhere.
Non-Financial Businesses and Professions

Casinos and Other Businesses Associated with Gambling

Casinos are among the most proficient cash-generating businesses. High rollers, big stakes, credit facilities, “comps,” and a variety of other factors combine to create a glittering amount of cash that flows from house to players and back. It reaches into the billions of dollars in the places it is legally permitted.

Casinos and other businesses associated with gambling, such as bookmaking, lotteries and horse races, continue to be associated with money laundering, since 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 occurs generally in the placement stage, i.e. converting the funds to be laundered from cash to checks. A launderer can buy chips with cash generated by a crime and then request repayment by 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, the FATF says that gaming businesses and lotteries too are being used increasingly by launderers. The group gives examples of multiple financial transactions made by the same person by way of checks drawn on gambling agencies, such as lotto, horse-racing and casinos. Circuits have been set up to organize systematic buy-back of winning tickets from their legitimate holders. A 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 more or less recovering his stake in the form of checks issued by the gambling or betting agency and corresponding to perfectly verifiable winnings from gaming. This method is much more reliable than the previous one, since the police investigation
service, once it has verified the reality of the gaming operation and the person’s winnings, will in principle have a great deal of trouble in going further and identifying the source of the money staked.

**Real-Life Example**
On October 20, 1988, Waldemar Ratzlaf, an inveterate 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 the $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 vicepresident told Ratzlaf to contact his bank in Oregon and make arrangements to obtain a cashier’s check, which would be gladly accepted. To ease the pain the casino provided a limousine and driver to assist in the banking transaction. The next day, accompanied by a casino employee, Ratzlaf and his wife went to 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 paid their casino debt. Then the Internal Revenue Service stepped in. The Ratzlafs told an inquiring IRS agent the cash represented gambling winnings and that the High Sierra casino had told them to “pay off the marker” with cashier’s checks in small amounts so that no currency transaction report would be required. 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 counts, 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 highvalue items within anti-money laundering monitoring systems. However, in many other jurisdictions, including the United States, these industries are yet to be regulated for money laundering control purposes.
Gold is attractive to money launderers. It has high intrinsic value in a relatively compact form, which is easy to transport. It can be bought and sold easily for currency in most areas of the world. It is more readily accepted than precious stones, especially since it can be melted down in many 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 the demand for it in certain regions of the world.

The FATF says in its 2002-2003 typologies lists gold’s advantages to money launderers as its high intrinsic value, convertibility and potential anonymity in transfers. It is used both as a source of illegal funds to be laundered (through smuggling or illegal trade in gold) and as a laundering vehicle (through the outright purchase of gold with illegal funds). Most laundering involving gold is linked to illegal narcotics trafficking, organized crime and illegal trade in merchandise. The gold itself may be the “proceeds” of crime that needs to be laundered. The FATF provides 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 then sold to a gold working company in Country F, which in turn forwarded its payments to the sellers’ accounts. Debits were regularly made from these accounts to accounts in another 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. The case was transmitted to the public prosecutor’s office, which is working with foreign authorities to dismantle the operations.
The FATF mentions another, more complex typology using the gold or precious metal purchases and sales as a cover for a laundering operation. 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 is also common to the various value-added tax fraud schemes, which are associated with gold-trafficking.

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 is vulnerable. The “dealer in precious metal” is being used to transfer an asset not only from one form into another — i.e. unrefined gold to refined gold or money within the international finance system — but also from one person to another.

- Precious metal pool accounts — These 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, and can be drawn on by that customer for return of that precious metal, or for sale and return of monetary proceeds, or for delivery of precious metal to another person. 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 telling their U.S. employees to buy precious stones in New York with drug proceeds, then 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 resell them to refiners for “clean” cash. According to the charges, the jewelers willingly accepted some $1 million in drug funds from undercover agents. They offered to smelt the gold into small objects, such as belt buckles, screws and wrenches, to facilitate smuggling them 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.

The U.S. Government Accountability Office reported in 2003 that diamonds and other gems are ideal for earning, moving and storing terrorist assets as alternative value transfer mechanisms. It cited expert reports that al Qaeda was buying so-called conflict diamonds from West African rebel groups in the months before 9/11 and may still be involved in the diamond trade. In August 2004, however, the 9/11 Commission Staff Monograph on Terrorist Financing disputed the theory that al Qaeda profited from conflict diamonds: “No persuasive evidence exists that al Qaeda had any substantial involvement with conflict diamonds.”

Individuals and entities in the diamond sector have been involved in complex diamond-related money laundering cases. As with gold, the simplest typology involving diamonds consists of direct purchase of the gems with ill-gotten money. The FATF says that the more common types of laundering activity related to this sector include retail foreign exchange transactions, 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 smokescreen for laundering proceeds generated by other criminal activity.

The multi-million-dollar fine art industry can also serve as a convenient money laundering vehicle. That has not escaped
drug traffickers and other criminals who must disguise illicit proceeds. 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**
A drug money laundering case in which priceless paintings of Goya and Foujita were involved illustrates this dark side of the art world. In 1998, Doris Salazar approached four Colombian drug traffickers to say she knew Saudi Arabian prince Nayef bin Sultan bin Fawwaz Al-Shaalan, who could transport cocaine anywhere in the world using his diplomatic status and personal jet. Al-Shaalan assured the Colombians he could safely transport 2.2 tons of cocaine from Venezuela to France. A plan began to take shape. In the next year Salazar, the Colombians and two others, Jose Clemente and Ivan Vanegas, attended meetings around the world to finalize the plan. In May 1999, the cocaine arrived in France. Here’s where the art comes in — and it gets tricky. While all four defendants are charged with drug trafficking, only Salazar has been arrested. Al-Shaalan, Vanegas and Clemente, the person charged with laundering conspiracy, remain at large (Title 18, USC Sec. 1956(h)). At this point, information about them and the laundering aspects of the case are limited. The media said Clemente tried to repay a supplier by transferring the two paintings as part of a laundering conspiracy. The U.S. money laundering law subjects property involved in the offense to forfeiture. The original paintings by Foujita, titled Buste de Jeune, and by Goya titled Bandits Attacking a Coach, were examined by a New York appraiser who concluded they were legitimate and worth about $1 million each. Both were seized. It’s likely the Drug Enforcement Administration (DEA) will request they be sold at auction with the money going to the government. It would not be the first time high-profile art and laundering crossed paths. In 2001, Boston art dealers Shirley Sack and Arnold Katzen were indicted for laundering after trying to sell two paintings by Modigliani and Degas for $4.1 million to an undercover agent posing as a drug dealer. The duo told the agent they could resell the paintings overseas as part of a laundering scheme. Another famous case was Operation Dinero, a 1992 joint DEA and IRS operation. The agencies operated a bank in Anguilla targeting the financial networks of international drug traffickers. Several undercover companies were established in different jurisdictions as fronts designed to supply laundering
services to the traffickers. Members of the Cali cartel fell for the bait and engaged 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: ƒÞ Require all art vendors to provide names and addresses. Ask that they sign and date a form that states the item is not stolen and that they are authorized to sell it. ƒÞ Verify the identities and addresses of new vendors and customers. Be suspicious of any item whose asking price does not equate to its market value. ƒÞ 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 stolen by enforcement agencies, insurers and individuals. It would not be the first time high-profile art and laundering crossed paths. In 2001, Boston art dealers Shirley Sack and Arnold Katzen were indicted for laundering after trying to sell two paintings by Modigliani and Degas for $4.1 million to an undercover agent posing as a drug dealer. The duo told the agent they could resell the paintings overseas as part of a laundering scheme.

Another famous case was Operation Dinero, a 1992 joint DEA and IRS operation. The agencies operated a bank in Anguilla targeting the financial networks of international drug traffickers. Several undercover companies were established in different jurisdictions as fronts designed to supply laundering services to the traffickers. Members of the Cali cartel fell for the bait and engaged 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 the item is 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 does not equate to 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 stolen by enforcement agencies, insurers and individuals.

- Look critically when a customer asks to pay in cash. Avoid accepting cash payments unless there is a strong and reputable reason to do so.
- Be aware of money laundering regulations.
- Appoint a senior staff member to whom employees can report suspicious activities.

**Travel Agencies**

Using a front, the launderer can mix illegal funds with legitimate money to make illegal funds look legitimate. For example, a travel agency that sends money to the Dominican Republic to allegedly arrange vacations might be sending additional money for criminal activities.

**Real-Life Case**

Named for the famous Ecuadorean mountain, Operation Chimborazo 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, the 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 raids in one of the countries, in Argentina, the authorities arrested 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 outgoing wire transfers in small amounts to avoid recordkeeping requirements, especially those from foreign countries and unusually large amounts
- Sending a tour group to a country and making an offsetting payment in a foreign entity’s U.S. or other account while instructing the accountholder to cover the cost of the group’s trip
- Arranging complex payment or invoicing for customers, thereby structuring cash payments to avoid currency reports.
**Vehicle Sellers**

This industry includes sellers and brokers of new land-based 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 structured checks and money orders
- Trading in vehicles for other ones and conducting successive transactions of buying and selling new and used vehicles to produce complex transaction layers
- Arranging complex payment or invoicing for customers, thereby structuring cash payments to avoid currency reports
- Accepting third-party payments, particularly from jurisdictions with lax laundering controls.

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

**Real Life Case**

In January 1993 ten car dealerships and 19 individuals were indicted in the Washington, D.C., area in the largest bust of businesses for money laundering since the cash reporting law took effect in 1985. Four additional individuals and one additional dealership were indicted for money laundering. Import Cars of Maryland Inc., which does business as Lane Honda College Park and salesmen and managers from Rosenthal Acura, Nissan-Mazda and Toyota allegedly accepted large amounts of cash from undercover FBI and IRS agents for cars that were supposedly being bought for drug cartels in Colombia. The agents allegedly told the managers they wanted to buy the vehicles to transport more drugs, reward workers who were helping them deal drugs and launder the cash from their drug sales. The government was seeking forfeiture of 55 cars in addition to the original 60, an estimated total value of $2.9 million. Dozens of individuals and six corporations were indicted in the undercover operation called Money Magic. As part of the FBI sting agents requested no cash reporting forms be filed.
Allegedly the dealership employees complied. They agreed to register the vehicles using fictitious names and to either prepare false reporting forms or none at all. The employees were paid “tips” for their role in the scheme.

There have also been cases where authorities charged that a car dealer laundered money by allowing a drug dealer to trade in his cars for cheaper models and walk away with checks, not cash, for the difference. In a “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 the customer was a drug dealer, in violation of the money laundering law. In this case there were also structuring charges against the car dealer and the company’s comptroller, stemming from the more than $19,000 remaining after the Porsche-for-Bronco trade. The two men disbursed the balance to the buyer in three separate checks. Each was for less than $10,000 allegedly to help the drug dealer avoid a currency transaction report.

**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 can either block or facilitate the entry of organized crime money into the financial system.

Those responsibilities include requiring gatekeepers such as lawyers to identify clients whose activities might involve money laundering, conduct due diligence on their clients, maintain records about clients and report “suspicious” client activities. Some of these rules also restrict lawyers from informing or “tipping off” clients who are the subjects of the suspicious activity reports. Violations may subject lawyers to prosecution, fines and even imprisonment.

In the European Union and several other countries mandatory antimoney 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, the FATF says that the following functions provided by lawyers, notaries, accountants and other professionals are the most useful to a potential money launderer:

- Creation of corporate vehicles or other complex legal arrangements (trusts, for example). Such constructions 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 laundering process (integration stage).
- Performing financial transactions. Sometimes these professionals may carry out various financial operations on behalf of the client (for example, cash deposits or withdrawals on accounts, retail foreign exchange operations, issuing and cashing checks, purchase and sale of stock, and sending and receiving international funds transfers.)
- Financial and tax advice. Criminals with large amounts 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.
- Gaining introductions to financial institutions.

The 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, one being both a lawyer and an accountant. The prosecution alleged 123 violations involving conspiracy, false claims, wire fraud and money laundering. The false claims involved fictitious patient claims and claims for services that were not provided.

The two primary subjects employed the lawyer’s services to set up four related shell corporations as the controlling entities. In addition, eight nominee corporations were created to generate fictitious health care service records reflecting home therapy and nursing care. Health care providers including therapists, registered nurses and physicians operated the nominee 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 US$4 million was laundered through bank accounts in cities of the north and southeast of the country and through suspected offshore accounts. Numerous accounts were created at four or five separate banks for purposes of amassing and moving these funds. Cashier’s checks often were purchased and even negotiated through the lawyer/accountant’s trust account for concealment of property acquisition.

The defendant was sentenced to two years in exchange for cooperation. Both primary defendants forfeited real and personal property, including the US$4 million and purchased property. They received five- and two-year prison sentences, respectively. Two additional related case defendants (one an elected official), laundered another US$2 million and were charged with 33 violations in a separate case. They were ordered to forfeit US$95,000. The former elected official received a five-year prison sentence.

In the United States, American Bar Association (ABA) and other lawyers’ groups are fighting money laundering regulations for their industry. The ABA urges the government “to seek to protect and uphold the attorney/client relationship, including the attorney/client privilege, in dealing with international money laundering.” It underscores “the growing threat to the attorney/client relationship, and specifically to the attorney/client privilege, by emerging international obligations (e.g., gatekeeper responsibilities) imposed on an array of professionals in an effort to curb and root out money laundering.” They say long-held principles of confidentiality “have been the hallmark of the relationship between attorneys and their clients in the United States.” It urged the government “to uphold and protect these principles in becoming a party to any international agreements or enacting legislation with respect to money laundering measures.”

The U.S. and the FATF are exploring various options under which they can:

- Defer regulation until adequate education is conducted.
- Impose internal controls and due diligence duties on lawyers, as the United Kingdom does through reporting exceptions for communication that is litigation-related.
• Utilize 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.
• Devise a new “hybrid” approach, such as through “guidance notes” or best practices standards from the FATF.

The initial gatekeeper battles in the U.S. will focus on the scope of the requirements, particularly the definition of the financial transactions to which reporting requirements would apply. Many regulators 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 subjects lawyers who conduct international transactions to their requirements.

**Investment and Commodity Advisors**

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

- **Commodity**: Goods such as food, grains and metals that are usually traded in large amounts on a commodities exchange, usually through futures contracts.
- **Commodity pool**: Combines funds from various members and uses them to trade in futures or options contracts.
- **Futures/futures contract**: A contract to buy or sell a quantity of a commodity at a future date at a set price.
- **Omnibus account**: An account 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 contract**: 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 advisors are persons who, for compensation or profit, 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 issues analyses or reports concerning trading futures or commodity options. Because they direct such accounts they 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 implement a compliance program to deter and detect 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 advisor 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, for compensation, 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 or withdrawals from accounts
- Checks drawn on, or wire transfers from, accounts of third parties with no relation to the client
- Clients who require 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 originator.
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-1980’s. The goals of Capcom were allegedly the misappropriation of BCCI assets for personal enrichment. That 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 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 by 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 in 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 and 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 accommodation, correspondence or administrative address 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,” the FATF states 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 outside of that client’s jurisdiction (e.g. a yacht, a residential or commercial property etc). Some TCSPs are required to afford confidentiality privileges to a client, which can conflict with AML reporting requirements, states the FATF.

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. They can monitor and, in some cases control, what is going on.
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 provided by the provider are to meet their obligations as trustees or trusteeships.

Transparency International says in its 2004 report that the first jurisdiction to bring these activities under regulatory control was Gibraltar, which enacted legislation in 1989. Other offshore jurisdictions have also either introduced some form of regulatory control or have plans to do so. Regulations are not uniform and 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 Know Your Customer (KYC) provisions virtually impossible. Furthermore, while some jurisdictions brought service provision within their anti-money laundering regulations — for example by making compliance with the regulations a condition of licensing — many did 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 was easy for a person seeking to use a company or trust for criminal purposes to select a jurisdiction that either lacked requirements or had only inadequate ones, says Transparency International.

**Real Estate Industry**

The real estate sector is fully within the sphere of money laundering activities. The several laundering cases that have involved use of criminal proceeds in real estate transactions argue strongly for including the sector under the anti-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 RCMP Cases,” nearly 56% of money laundering or proceeds of crime cases investigated by the Royal Canadian Mounted Police involve real estate. The report says that deposit institutions and real estate firms constitute 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 to property through such transactions as deposits, down payments, mortgages, lawyers’ trust accounts and even through construction. The use of nominees, who hide the identity of the true beneficial owner, was found in 46.3% of the cases, making it the most popular laundering technique.

Laundering may be accomplished either by way of chain transactions in real estate to cloak 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, the 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 US$ 4.4 million was confiscated.

Real-Life Case
Marbella, the Mediterranean resort for the well-heeled on Spain’s Costa del Sol, is acquiring a new label as headquarters for a vast criminal network that laundered more than 250 million euros through front companies and real estate investments. An extensive investigation called Operation White Whale, led by the Spanish Policía Nacional, yielded 50 arrests, the freezing of hundreds of bank accounts and the seizure of 410,000 euros, dozens of luxury cars, a ship and two private airplanes. It is being called Spain’s largest-ever money laundering case. In mid-April 2005, Judge Miguel Angel Torres placed Mario Blanco, manager of several Costa del Sol real estate investment companies, in preventive custody. Spanish lawyer Jorge Poggio, who has ties to more than 20 real estate agencies, was freed on bail. Both were detained for alleged money laundering through real estate holdings in Spain through a company Allerteen Holdings S.L.
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 payment of the proceeds to the seller, payoff of mortgage, real estate commissions, taxes, satisfaction of liens and other payments. Title insurance agencies often obtain cashier’s checks for those types of disbursements.

To a bank and other observers, the disbursement of funds at a closing appears to be all one legitimate transaction. Money laundering can be hidden because the size and volume of routine escrow account activity smooths out the “spikes” (which describe sudden ups and downs in an account) or multiple deposits associated with money laundering. Escrow accounts provide a rationale and method for circumventing cash reporting requirements. They also 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 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, you should take notice. These manipulated trade prices represent money laundering, tax evasion 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, 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, they can detect abnormal pricing schemes involving every commodity that leaves or enters the U.S. They say over-pricing or under-pricing imports and exports facilitates tax evasion, money laundering and terrorist financing. The professors say the favorite 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,” the FATF defines 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, states the FATF. 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 concludes 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, in Europe) derived from illegal activity is purchased by Colombian (and other countries’) “peso brokers” from criminals in other countries 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 utilizing 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 has issued advisories to U.S. financial institutions and corporations seeking help in combating this billion-dollar currency exchange and money laundering network.

For financial institutions to detect and prevent laundering by peso brokers, they must be familiar with the common laundering methods the brokers use. 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 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. Ultimately, in August 2000, the helicopter in question was seized in Panama on grounds that it had been paid for with drug money.

Source: United States Department of Homeland Security

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 electronically means.
**Online or Internet Banking**

Many financial institutions offer customers Internet accounts, with the same 24-hour services as those offered at the counter. They permit “virtual counters” permitting 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, the FATF says 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 since the traditional methods of supervision cannot be applied, says the FATF.

The greatest 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 an elimination of face-to-face contact between customer and employee, will necessarily make it more difficult to know who is actually controlling the account
- The ease of access through the Internet
- The rapidity of electronic transactions.

To combat cyberlaundering, the 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 be 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. The FATF says anyone can access an open account online, and verifying the identity of the person who accesses the account may not be possible.

This problem is complicated by the fact that some servers do not use “log files” to trace the origin of the computer through which a transaction is made. Thus, the Internet-protocol number of the server and the date and time of connection are not kept in an electronic file. The roots of the transmissions are effectively kept private and virtually untraceable, says the FATF.

Online banking will attract money launderers because of its potential to aid them in the three classical 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, will 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 may not apply. Using “super smart-card” technologies, cash could be moved around the world through ATM transactions. These smart cards promise easy retrieval of the “account” balance by using an ATM card.

**Internet Casinos**
According to the FATF, Internet gambling might be an ideal webbased “service” to serve as a cover for a money laundering scheme. There is evidence in some FATF jurisdictions that criminals are using Internet gambling to commit crime and to launder criminal proceeds. Despite attempts to deal with the potential problems of Internet gambling by regulating it, requiring operating licenses, or banning such services outright, a number of concerns remain, in addition to the inability to track the Internet links mentioned above. 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. Furthermore, gambling transactions — the records of which might be needed as evidence — are conducted at the gambling site and are software-based; this may add to the difficulty of collecting and presenting such evidence.

According to the U.S. State Department’s 2003 International Narcotics Strategy Report, 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 email, violated 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. It was fortified by the USA Patriot Act to make it a crime for even 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). The U.S. Attorney in Eastern Missouri says PayPal transmitted illegal online gambling proceeds funds repeatedly. The prosecutor notified PayPal by a March 28, 2003, letter that it could be forced to forfeit its online gambling profits earned from October 26, 2001, to July 31, 2002, with interest. The company was also informed it could face criminal prosecution. In July 2002, PayPal turned over to a federal grand jury documents on its online gambling services. In August 2002, PayPal agreed with New York’s Attorney General to stop processing payments by New Yorkers to gambling merchants. It paid $200,000 in penalties and gave up its profits. PayPal stopped processing payments for online gambling companies in November 2002, a month after it was acquired by the online giant auctioneer, eBay. About 6% of PayPal's 2002 revenues came from online gambling merchants, according to eBay’s 2002 10K filing with the Securities and Exchange Commission. In that filing, eBay said PayPal “acted in the good faith belief that its conduct did not violate (the money laundering law).” Without disclosing its profits from online gaming, eBay said “the monetary amounts associated with this matter are not expected to have a material impact on our financial position, results of operations or cash flows.” Still, the company is wary of harm the accusations could cause. “Any finding of a civil or criminal violation by PayPal, or potentially any settlement, could also endanger PayPal’s ability to obtain, maintain or renew money transmitter licenses in jurisdictions where it requires such licenses to operate....,” the filing said. 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. Many bills have been filed to curb Internet gambling, but no measure has received final approval in the U.S.

Citibank, one of the largest issuers of credit cards in the United States, no longer allows use of its Visa or Mastercard credit cards for online gambling. Coupled with similar action by other
large credit card systems, the move decreased the money laundering opportunities through cyberspace.

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

In a submission to the FATF during its review of the FATF 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 realworld gambling facilities — is in a better 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 states. Whatever exposure the interactive gaming industry has to money laundering can be mitigated through rigorous regulation, the organization adds.

Nevertheless, online gambling provides an excellent method of laundering because transactions are conducted principally through credit or debit cards. Site operators are typically unregulated offshore firms, which opens the door to laundering and other criminal mischief. 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 is difficult for enforcement and regulatory agencies.

**Real-Life Case**

In 2004, Russian police charged three men with being members of a gang that extorted 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), which described the arrests as a joint Russian-British operation. The three men were detained in raids in St. Petersburg and in the Saratov and Stavropol regions of southwestern Russia. Police were led to the men after the arrests of 10 money laundering
“mules” in Latvia. According to press reports, police had followed a money trail from London, to the Caribbean, Latvia and then 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 for a year. One of the UK firms reportedly met the ransom demands after being advised by police to do so. Other UK firms spent as much as €151,000 beefing up security.

Prepaid Cards and E-Cash


In October 2006, the FATF published a report that examined the way 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 within a particular country. The report recommends 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’re 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, they 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 and 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 may not observe laws in all jurisdictions
- Substitute for bulk-cash smuggling

The prepaid cards’ rapid proliferation and lacking regulatory clarity in the United States prompted money services businesses to ask regulators to certify pre-paid card sellers, but regulators are still reluctant to saddle the burgeoning financial product with onerous regulations. 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 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 the memory chips.

The use of these payment systems has declined considerably over the past decade, according to the 2006 FATF report. Only one, the German GeldKarte, operates in multiple jurisdictions – Germany and Luxembourg – with a limit of €200 ($254).
The report identified these potential risk factors:
- Anonymous card holders
- Anonymous funding and access to funds
- High value limits
- No transaction records

Measures that might limit the vulnerability to money laundering of new payment technologies are:
- Limiting the functions and capacity of smart cards (including maximum value and turnover limits, as well as number of smart cards per customer);
- Linking new payment technology to financial institutions and bank accounts;
- Requiring standard record keeping procedures for these systems to enable the examination,
- Documentation, and seizure of relevant records by investigating authorities; and
- Establishing international standards for these measures.

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.

The 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 sold to someone who would prefer to have an existing corporation than a new one.

**Shell company/corporation:** A company that is incorporated that at the time has no significant assets or operations.

In October 2006 the FATF issued a report called “the Misuse of Corporate Vehicles, Including Trust and Company Service Providers.” The FATF says that of particular concern is 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 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 the FATF reviewed the rules and practices that impair the effectiveness of money laundering prevention and detection systems as part of its non-cooperative countries and territories initiative, it found in particular that:

*Shell corporations and nominees are widely used mechanisms to launder the proceeds from crime, particularly bribery (e.g. to build up slush funds). 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,” offers four related reasons to establish or control a company for money laundering purposes:

- Companies accomplish the objective of converting the cash proceeds of crime into alternative assets. This is most apparent with investments in an operating business with hard assets.

- Through the use of shell companies, the launderer can create the perception that illicit funds have been generated from a legitimate source. Once a 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.

Examples
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. A hotel is posting tremendous sales, according to its books, whereas in reality, it rarely has guests in its rooms. Its administrative and financial records, however, show an occupancy rate of almost 100%.

Since 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 dirty money. The dirty money is laundered by pretending it is revenue earned by these front companies. The criminal pays tax on the money.

Generally, front companies also have legitimate revenue, but sometimes their total revenue comes from money generated by crime. Then there is no real business going on anymore. In these cases, criminals may have the whole vertical business column in his power, from production to wholesale to retail.

- Once a 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, offering public shares in the company, or purchasing real estate with proceeds of crime disguised as mortgages issued by a shell company. As a medium between criminal organizations and other laundering vehicles, 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.

- 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. 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 real business apart from laundering. 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 held by professionals who claim secrecy; and the professionals who run the company act on instructions remotely and anonymously. Shell companies can easily be established with little start-up capital and no legitimate business.

Criminal enterprises also utilize 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. Once the shell or legitimate company is established, the primary objective of the company is to claim the proceeds of crime as legitimate revenue and/or commingle criminal proceeds with legitimate revenue (which is then most often deposited into a commercial bank account).

The Canadian report mentions the following other laundering techniques used in conjunction with criminal 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. Often, companies established by lawyers will be registered in their 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, the Canadian report says a Toronto drug trafficker had $500,000 in a bank account in the name of a shell company. These funds were re-invested in restaurants operated by the criminal enterprise and costing $1 million. A down payment of $50,000 in legitimate money was made and properly declared. A $450,000 mortgage was then negotiated from a bank. The remaining $500,000 was “borrowed” from the bank account of the criminal enterprise’s shell company. The $500,000 was repaid with interest to avoid suspicion.

- **Fictitious business expenses/False invoicing** — The report says that 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 Canada, and the payment is sent in full to the bank account of the Canadian 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 Canadian company has been charged a high price for the goods, the books of the Canadian company show a low level of profit, which means that company will also pay less in taxes. It can also work the other way around. An offshore corporation buys goods from a Canadian company at a price that is too high. The difference between the real price and the inflated price is then deposited in a numbered account in a tax haven country.

- **Sale of the business** — When the criminal sells the business, he has a legitimate source or 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 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 in 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 to Canada. Often, the business will be purchased at an artificially inflated price. The difference between the artificial and the real market value is deposited in the bank account of a foreign subsidiary company in a tax haven country. A reverse situation may occur where a Canadian company is sold at an artificially low price.

• **Paying out fictitious salaries** — In addition to claiming the proceeds of crime as legitimate business revenue, criminally-controlled companies also help legitimate certain participants in a criminal conspiracy by providing them with salaries. In some cases, salary checks were signed back to the company by the “employee” as part of the laundering operation.

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**
A trust is defined in the FATF’s 2000-2001 typologies report as a legal relationship that is set up – either “inter vivos,” or on death – by a person (the “settlor”) when the 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. Sometimes a trust might involve a fourth person, a trust protector, who is appointed by the settlor to ensure that the trustee manages or disposes of the assets held in trust according to the settlor’s intentions.

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...
the dirty 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, 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 could be used in the money laundering process, because these payments do not have to be justified as compensation for a transfer of assets or service rendered.

Lawyers often serve as nominees by holding money or assets “in trust” for clients. This enables lawyers to conduct transactions and administer the affairs of a client. Sometimes, the dirty money is placed in a law firm’s general trust account in a file set up in the name of the offender, a nominee, or a company controlled by the offender. 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, since there is no registry of owners, the transfer takes place by physically handing-over the bond or share certificate.

Bearer shares offer lots of opportunities to disguise their legitimate ownership. To prevent this from happening, the FATF, in its review of the 40 Recommendations, suggests that employees of financial institutions ask more questions about the identity of beneficial owners before issuing, accepting or creating bearer shares and trusts. The FATF paper does not specify the questions that should be asked. Financial institutions
should also keep registries of this information and share it appropriately with law enforcement agencies.

Several FATF members do allow 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 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**

One nation after another, many of them touched by the global investigation into bank accounts linked to the terrorist cells spearheaded by Osama bin Laden and other terrorist groups, have made commitments to break up internal elements of the financial networks that fund terrorism.

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 urging all nations to freeze the assets of known terrorists. Since then, many countries have committed to helping disrupt terrorist assets by alerting financial institutions to persons and organizations that authorities say are linked to terrorism.

The G-7 nations marshaled the Paris-based Financial Action Task Force (see also Chapter on International Standards), the organization they created in 1989 to combat global money laundering, to hold an “extraordinary plenary session” on October 29, 2001, in Washington.
Differences and Similarities Between Terrorist Financing and Money Laundering

Nowadays, money laundering and terrorist financing are often mentioned in the same breath, without much consideration to the critically important differences between the two. Even the controls that businesses must 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 little different from 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 help them distinguish suspicious terrorist financial activity from money laundering.

The most basic difference between terrorist financing and money laundering involves the origin of the funds in question. Terrorist financing uses funds for an illegal political purpose, but the money itself is not necessarily derived illegally. On the other hand, money laundering 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. With his analysis as a base and to assist in detecting those crimes, here is a more detailed look at the differences between two major world problems:

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, use of debit or credit cards. The hawala system has also a role in moving terrorist related funds. Also, money raised for terrorist groups are generally used for mundane expenses like food and rent, and not directly for the terrorist acts themselves.

**Money Laundering**
- **Motivation**: Profit
- **Source of Funds**: Internally from within criminal organizations
- **Conduits**: Favors formal financial system
- **Detection Focus**: Suspicious transactions, such as deposits uncharacteristic of customer’s wealth or the expected activity, which lead to relational links
- **Transaction Amounts**: Large amounts often structured to avoid reporting requirements
- **Financial Activity**: Complex web of transactions often involving shell or front companies, bearer shares, and offshore secrecy havens
- **Money Trail**: Circular — money eventually ends up with person who generated it

**Terrorist Financing**
- **Motivation**: Ideological
- **Source of Funds**: Internally from self-funding cells (increasingly centered on criminal activity)
- **Conduits**: Favors cash couriers or informal financial systems such as hawala and currency exchange firms
- **Detection Focus**: Suspicious relationships, such as wire transfers between seemingly unrelated parties, which lead to transactional links
- **Transaction Amounts**: Small amounts usually below reporting thresholds
- **Financial Activity**: No workable financial profile of operational terrorists exists, according to U.S. 9/11 Commission
- **Money Trail**: Linear — money generated is used to propagate terrorist group and activities

**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. They 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, let alone terrorists bent on mass murder. The money laundering controls in place at the time were largely focused on drug trafficking and large-scale financial fraud and could not have detected the hijackers’ transactions. The controls were never intended to, and could not, detect or disrupt the routine transactions in which the hijackers engaged.

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 or directly from Khalid Sheikh Mohamed (KSM) as they transited Pakistan before coming to the United States. The plot cost al Qaeda somewhere in the range of US $400,000–500,000, of which approximately $300,000 passed through the hijackers’ bank accounts in the United States. The hijackers returned approximately $26,000 to a facilitator in the UAE in the days before the attack. While in the United States, the hijackers spent money primarily for flight training, travel and living expenses (such as housing, food, cars, and auto insurance). Extensive investigation has revealed no substantial source of domestic financial support.

Through reconstruction of available financial information, the U.S. Internal Revenue Service and the Federal Bureau of Investigation established how the hijackers responsible for the Sept. 11 attacks received their money and how money was moved out of 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
The hijackers tended to open accounts in groups of three or four individuals
Some of the accounts were joint accounts
Addresses used usually were not permanent (i.e., mail boxes) and 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
Hijackers made numerous attempts of cash withdrawals that often exceeded the limit of the debit card
High percentage of withdrawals was from debit cards
Low percentage of checks was written
Numerous balance inquiries were made
After a deposit was made, withdrawals occurred immediately
There was no discernible pattern of timing of deposits/disbursements
Account transactions did not reflect normal living expenses for rent, utilities, auto payments, insurance, etc.
Funding for daily expenditures was not evident from transactions
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 (uninterrupted 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. These traveler’s checks were partially deposited into their U.S. checking accounts.
- Three of the hijackers (pilots/leaders) continued to maintain bank accounts in Germany after moving to the U.S.
- Two of the hijackers (pilots/leaders) had credit cards issued by German banks and maintained those cards after moving to the U.S.
- One of the hijackers (pilot/leader) received substantial funding through wire transfers into his German bank account in 1998 and 1999 from one individual.
- In 1999, this same hijacker opened an account in UAE, giving 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 to plumb the murky field of terrorist financing and offer recommendations to the world financial community, the FATF has issued guidance to identify techniques and mechanisms used in financing terrorism. The report “Guidance for Financial Institutions in Detecting Terrorist Financing,” published April 24, 2002, 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, the 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 these examples and others that it provides:
- Use of an account as a front for a person with suspected terrorist links revealed by a previous suspicious transaction report
- Appearance of an accountholder’s name on a list of suspected terrorists, such as that issued by the UN Security Council Committee on Afghanistan
- Companies that were subject to previous suspicious transaction reports and through which many funds transfers pass in a short time
- Frequent large cash deposits in accounts of non-profit organizations
- High account turnover in relation to accountholder’s salary
- Lack of clear relationship between banking activity and nature of accountholder’s business.

The FATF suggests that with these scenarios in mind, financial institutions should pay attention to these 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 or Asia, and commonly involve the international transfer of value outside the legitimate banking system. They are based on trust.

Hawala was born centuries before Western financial systems in India and China 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 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, with business people in various parts of the world using their corporate 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 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 a meager paper trail. The details of the customers who will receive the funds, which are usually minimal, are faxed between the brokers, and the customers obtain their funds from the brokers at each end of the transaction.

Below you can find a chart from Interpol that shows the Basic sequence of communication and payment in an alternative remittance:
Since 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 this cash in bank accounts. She will justify these deposits to bank officials as the proceeds of legitimate business. She may also use some of the cash received to pay for her business expenses, reducing her need to deposit the cash into the bank account.

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 could be layered to make following the money even more difficult. This could be done by using hawala brokers in several countries, and by distributing the transfers over time. Hawala techniques are capable of transforming 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 could 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 potential government oversight and do not keep detailed records in standard form. Although hawaladars do keep ledgers, their records are often written in idiosyncratic shorthand and maintained only briefly.

Al Qaeda moved much of its money by hawala before 9/11. In some ways, al Qaeda had no choice after its move to Afghanistan in 1996; the banking system there was unreliable. Bin Laden turned to an established hawala network operating in Pakistan, Dubai and throughout the Middle East to transfer funds efficiently. Al Qaeda used about a dozen trusted hawaladars, 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 deal.

**Real-Life Case**
Al-Barakaat (literally, “the blessing”), a moneyremitting system centered in Somalia with outlets worldwide, took shape after the
collapse of the Somali government and banking system. The intelligence community developed information that Osama Bin Laden had contributed money to al-Barakaat to start operations, that it was closely associated with or controlled by the terrorist group Al-Itihaad Al-Islamiya (AIAI), and that some of al-Barakaat’s proceeds went to fund AIAI, which in turn gave a portion to Bin Laden. In the U.S. the FBI developed an intelligence case on the al-Barakaat network in early 1999, and had opened a criminal case by 2000. Shortly after 9/11 al-Barakaat’s assets were frozen and its books and records were seized in raids around the world. Subsequent investigation by the FBI, including financial analysis of the books and records of al-Barakaat provided in unprecedented cooperation by the United Arab Emirates, failed to establish allegations of a link between al-Barakaat and AIAI or Bin Laden. No criminal case was made against al-Barakaat in the United States for these activities. Although the U.S. Office of Foreign Assets Control (OFAC) claims that the freeze met the evidentiary standard for designations, the majority of assets frozen in the United States under executive order (and some assets frozen by other countries under UN resolution) were unfrozen and the money returned after U.S.-based al-Barakaat money remitters filed a lawsuit challenging the action. (Source: Monograph on Terrorist Financing, the National Commission on Terrorist Attacks Upon the United States, 2004)

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 become targets of what they claim are unfair investigations or accusations.

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

- Enjoy the public trust
- Have access to considerable sources of funds
- Are often cash-intensive.
• Often have a global presence, often exactly in or next to those areas that are most exposed to terrorist activity.
• Often are subject to little or no regulation or have few obstacles to their creation.

To help legitimate non-profit organizations avoid ties to terrorist-related entities and regain public trust, the Financial Action Task Force issued guidelines in 2002 on charitable best practices for 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 bank accounts and foreign offices. The 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

The FATF recommends charities use formal bank accounts to store and transfer funds so 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.

The crime of money laundering also comprises the movement of funds to support terrorism or terrorist organizations. These 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, securities and insurance industry.

New payment technologies, including prepaid cards, online banking and electronic cash, can widen the opportunities for laundering. If an online financial institution is located in an area known for high levels of banking secrecy and requires little or no proof of identity for opening an account, the money launderer can move funds from his personal computer. 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?
- Why is private banking so vulnerable to money laundering?
- What are PTAs and what makes them vulnerable to money laundering?