STUDY GUIDE

CAMS CERTIFICATION EXAM

A PUBLICATION OF

ACAMS® | Advancing Financial Crime Professionals Worldwide®

acams.org

STUDY GUIDE

CAMS CERTIFICATION EXAM

A PUBLICATION OF

ACAMS® Advancing Financial Crime Professionals Worldwide®

acams.org

STUDY GUIDE
CAMS CERTIFICATION EXAM

SIXTH EDITION

Executive Vice President
John J. Byrne, CAMS

Project Manager
Catalina Martinez

We would like to thank the following individuals for their significant contribution
in the development of the CAMS Examination and Study Guide
through the work of the CAMS Examination Task Force.

Bob Pasley, CAMS—*Task Force Chair*
Kevin Anderson, CAMS—*Task Force Chair*
Brian Stoeckert, CAMS—*Task Force Chair*
Paul Osborne, CAMS—*Task Force Chair*
Peter Wild, CAMS-Audit—*Task Force Vice Chair*
Barbara Keller, CAMS—*Task Force Vice Chair*
Hue Dang, CAMS-Audit *(ACAMS Asia)*
Samantha Sheen, CAMS *(ACAMS Europe)*
Rick Small, CAMS—*ACAMS Advisory Board*
Nancy Saur, CAMS—*ACAMS Advisory Board*
David Clark, CAMS—*ACAMS Advisory Board*
Vasilios Chrisos, CAMS—*ACAMS Advisory Board*
Anna Rentschler, CAMS—*ACAMS Advisory Board*
Dennis Lormel, CAMS—*ACAMS Advisory Board*

Abbas Bou Diab, CAMS
Angel Nguyen, CAMS
Brian Vitale, CAMS-Audit
Brigette K. Miller, CAMS
Christopher Bagnall, CAMS
Christopher Randle, CAMS-Audit, CAMS-FCI
Dave Dekkers, CAMS-Audit
Deborah Hitzeroth, CAMS-FCI
Donna Davidek, CAMS-Audit
Ed Beemer, CAMS-FCI
Eric Wathen, CAMS
Gary Bagliebter, CAMS
Iris Smith, CAMS-Audit
Iwona Skornicka Castro, CAMS
Jack Sonnenschein, CAMS-Audit
Jeremy Brierley, CAMS
Jim Vilker, CAMS
Joel Conaty
Jurgen Egberink, CAMS
Kenneth Simmons, CAMS-Audit
Kok Cheong Leong, CAMS-Audit
Lauren Kohr, CAMS-Audit
Lindsay Dastrup, CAMS-Audit
Margaret Silvers, CAMS
Martin Dilly, CAMS-Audit
Nancy Lake, CAMS-Audit, CAMS-FCI
Peter Warrack, CAMS
Rachele Byrne, CAMS
Sean McCrossan, CAMS-FCI
Sharon McCullough, CAMS
Steve Gurdak, CAMS
Susan Cannon, CAMS-Audit
Susanne Wai Yin Ong, CAMS
Tatiana Turculet, CAMS
Venus Edano, CAMS
William Aubrey Chapman, CAMS-Audit
Yevgeniya Balyasna-Hooghiemstra, CAMS
Zachary Miller, CAMS-FCI

ACAMS would also like to thank the ACAMS Chapters worldwide
for their contribution in the development of the CAMS Examination.

Special Contributor: Gina Storelli, CAMS-Audit

 ISBN: 978-0-9777495-2-2

Table of Contents

Introduction

Chapter 1

About ACAMS

The mission of ACAMS is to advance the professional knowledge, skills and experience of those dedicated to the detection and prevention of money laundering around the world, and to promote the development and implementation of sound anti-money laundering policies and procedures. ACAMS achieves its mission through:

- Promoting international standards for the detection and prevention of money laundering and terrorist financing;
- Educating professionals in private and government organizations about these standards and the strategies and practices required to meet them;
- Certifying the achievements of its members; and
- Providing networking platforms through which AML/CFT professionals can collaborate with their peers throughout the world.

ACAMS sets professional standards for anti-financial crime practitioners worldwide and offers them career development and networking opportunities. In particular, ACAMS seeks to:

- Help AML professionals with career enhancement through cutting-edge education, certification and training. ACAMS acts as a forum where professionals can exchange strategies and ideas.
- Assist practitioners in developing, implementing and upholding proven, sound AML practices and procedures.
- Help financial and non-financial institutions identify and locate Certified Anti-Money Laundering Specialists (CAMS) designated individuals in the rapidly expanding AML field.

ABOUT THE CAMS DESIGNATION

As money laundering and terrorist financing threaten financial and non-financial institutions and societies as a whole, the challenge and the need to develop experts in preventing and detecting financial crime intensifies. ACAMS is the global leader in responding to that need, having helped standardize AML expertise by creating the CAMS designation.

Internationally-recognized, the CAMS credential identifies those who earn it as possessing specialized AML knowledge. AML professionals who earn the CAMS designation position themselves to be leaders in the industry and valuable assets to their organizations.

Congratulations on your decision to pursue the most respected and widely recognized international credential in the AML field. We welcome and invite you to embark on a journey that may lead you to career advancement, international recognition and respect among peers and superiors.

Read on, study hard and good luck!

Chapter 1

Risks and Methods of Money Laundering and Terrorist Financing

What is Money Laundering?

Money laundering involves taking criminal proceeds and disguising their illegal sources in order to use the funds to perform legal or illegal activities. Simply put, money laundering is the process of making dirty money look clean.

When a criminal activity generates substantial profits, the individual or group involved must find a way to use the funds without drawing attention to the underlying activity or persons involved in generating such profits. Criminals achieve this goal by disguising the source of funds, changing the form or moving the money to a place where it is less likely to attract attention. Criminal activities that lead to money laundering (i.e., predicate crimes) can include: illegal arms sales, narcotics trafficking, contraband smuggling and other activities related to organized crime, embezzlement, insider trading, bribery and computer fraud schemes.

Formed in 1989, the Financial Action Task Force (FATF) is an inter-governmental body comprising the Group of Seven industrialized nations to set standards and foster international action against money laundering. One of FATF's early accomplishments was to dispel the notion that money laundering is only about cash transactions. Through several money laundering "typologies" exercises, FATF demonstrated that money laundering can be achieved through virtually every medium, financial institution or business.

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

- 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 or her actions.
- The concealment or disguise 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.

An important prerequisite in the definition of money laundering is "knowledge." In all three of the bullet points mentioned above, we see the phrase "…knowing that it is derived from a criminal offense," and a broad interpretation of "knowing" is generally applied. In fact, FATF's 40 Recommendations on Money Laundering and Terrorist Financing and the 4th European Union Directive on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing (2015) state that the intent and knowledge required to prove the offense of money laundering includes the concept that such a mental state may be inferred from "objective factual circumstances."

A number of jurisdictions also use the legal principle of "willful blindness" in money laundering cases to prove knowledge. Courts define willful blindness as the "deliberate avoidance of knowledge of the facts" or "purposeful indifference" and 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.

After the events on September 11, 2001, in October 2001, FATF expanded its mandate to cover the financing of terrorism. Both terrorists and money launderers may use the same methods to move their money in ways to avoid detection, such as structuring payments to avoid reporting and use of underground banking or value transfer systems such as hawala, hundi, or fei ch'ien. However, whereas funds destined for money laundering are derived from criminal activities, such as drug trafficking and fraud, terrorist financing may include funds from perfectly legitimate sources. Concealment of funds used for terrorism is primarily designed to hide the purpose for which these funds are used, rather than their source. Terrorist funds may be used for operating expenses, including paying for food, transportation and rent, as well as for the actual material support of terrorist acts. Terrorists, similar to criminal enterprises, covet the secrecy of transactions regarding their destination and purpose.

In February, 2012 FATF modified its initial list of recommendations and notes into a new list of 40 recommendations, which include a new recommendation addressing ways to prevent, suppress and disrupt the proliferation of weapons of mass destruction.

Three Stages in the Money Laundering Cycle

Money laundering often involves a complex series of transactions that are difficult to separate. However, it is common to think of money laundering as occurring in three stages:

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

During this phase, the money launderer introduces the illicit proceeds into the financial system. Often, this is accomplished by placing the funds into circulation through formal financial institutions, casinos, and other legitimate businesses, both domestic and international.

Examples of placement transactions include:

- Blending of funds: Commingling of illegitimate funds with legitimate funds such as placing the cash from illegal narcotics sales into cash-intensive locally owned restaurant
- Foreign exchange: Purchasing of foreign exchange with illegal funds

- Breaking up amounts: Placing cash in small amounts and depositing them into numerous bank accounts in an attempt to evade reporting requirements
- Currency smuggling: Cross-border physical movement of cash or monetary instruments
- Loans: Repayment of legitimate loans using laundered cash

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

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

Examples of layering transactions include:

- Electronically moving funds from one country to another and dividing them into advanced financial options and or markets
- Moving funds from one financial institution to another or within accounts at the same institution
- Converting the cash placed into monetary instruments
- Reselling high value goods and prepaid access/stored value products
- Investing in real estate and other legitimate businesses
- Placing money in stocks, bonds or life insurance products
- Using shell companies to obscure the ultimate beneficial owner and assets

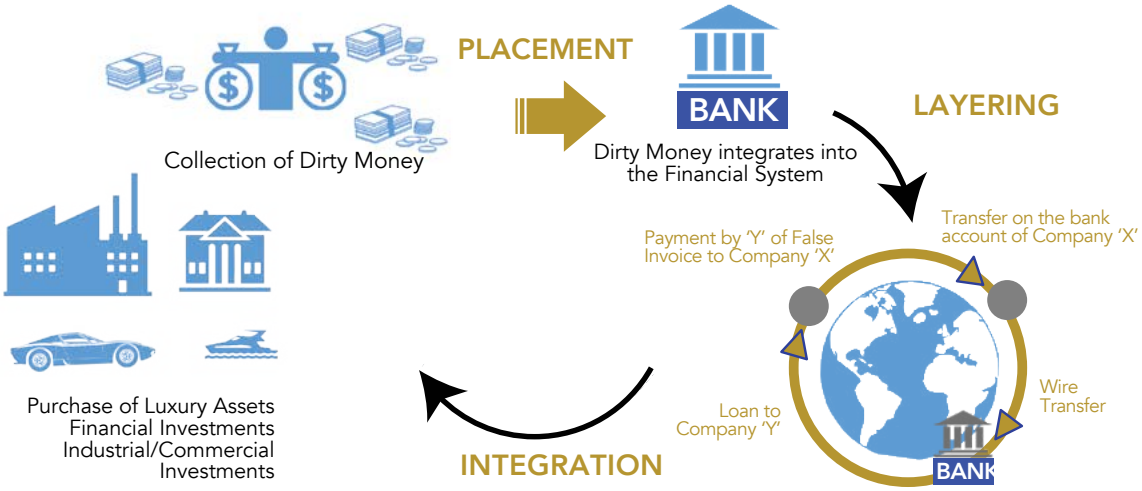
Stage Three: Integration — Supplying apparent legitimacy to illicit wealth through the re-entry of the funds into the economy in what appears to be normal business or personal transactions.

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

Examples of integration transactions include:

- Purchasing luxury assets like property, artwork, jewelry or high end automobiles
- Getting into financial arrangements or other ventures where investments can be made in business enterprises

Stages of Money Laundering



Source: The United Nations, Office of Drugs and Crime

The Economic and Social Consequences of Money Laundering

Money laundering is a result of any crime that generates profits for the criminals involved. It knows no boundaries and jurisdictions where there are weak, ineffective or inadequate anti-money laundering (AML) and counter-terrorism financing (CFT) legislation and regulations are most vulnerable. However, large, well-developed financial centers are also vulnerable to laundering due to the large volumes of transactions that allow the launderer to blend in and the wide range of services that enable the launderer to conduct transactions in a way that is convenient. Since most launderers want to eventually use the proceeds of their crimes, their ultimate intent is to move funds through stable financial systems.

Money laundering has significant economic and social consequences, especially for developing countries and emerging markets. The easy passage of funds from one institution, or relatively facile systems that allows money to be placed without raising any questions, is fertile territory for money launderers. The upholding of legal, professional and ethical standards is critical to the integrity of financial markets.

The potential macroeconomic consequences of unchecked money laundering include:

- **Increased Exposure to Organized Crime and Corruption:** Successful money laundering enhances the profitable aspects of criminal activity. When a country is seen as a haven for money laundering, it will attract people who commit crime. Typically, havens for money laundering and terrorist financing have:
  - — Limited numbers of predicate crimes for money laundering (i.e., criminal offenses that may permit a jurisdiction to bring a money laundering charge).
  - — Limited types of institutions and persons covered by money laundering laws and regulations.

— Little to no enforcement of the laws, and weak penalties or provisions that make it difficult to confiscate or freeze assets related to money laundering.

— Limited regulatory capacity to effectively monitor and supervise compliance to money laundering and terrorist financing laws and regulations.

If money laundering is prevalent, there is more likely to be corruption. Typically, the penetration of organized crime groups in a jurisdiction is directly linked to public and private sector corruption. Criminals may try to bribe government officials, lawyers and employees of financial or non-financial institutions so that they can continue to run their criminal businesses.

In countries with weaker laws and enforcement, it is corruption that triggers money laundering. It also leads to increases in the use of bribery in financial institutions, amongst lawyers and accountants, the legislature, enforcement agencies, police and supervisory authorities, and even with courts and prosecutors.

A comprehensive AML/CFT framework on the other hand helps curb criminal activities, eliminates profits from such activities, discourages criminals from operating in a country especially where law is enforced fully and proceeds from crime are confiscated.

Case Study

A US National Security Council report in 2001 found that Russian organizations were taking advantage of Israel's large Russian immigrant community to illegally produce compact discs or CDs and launder the proceeds. Israel gained a reputation as being "good for money laundering" amongst Russian gangsters. Israeli police estimated that more than US$4 billion of dirty money poured into Israel, others estimated it at about US$20 billion. These criminal gangs bought large parcels of land in impoverished development towns, taking over everything from local charities to the town hall, even handpicking several candidates for local and national offices. This further entrenched the gangsters, ensuring they got the benefit of policies and protection from authorities.

- **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: businesses that appear legitimate and engage in legitimate business but are in fact controlled by criminals who commingle the proceeds of illicit activity with legitimate funds to hide the ill-gotten gains. These front companies have a competitive advantage over legitimate firms as they have access to substantial illicit funds, allowing them to subsidize products and services sold at below market rates. This makes it difficult for legitimate businesses to compete against front companies. Clearly, the management principles of these criminal enterprises are not consistent with traditional free market principles, 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 taxes, thus depriving the country of revenue.

- **Weakening Financial Institutions:** Money laundering and terrorist financing can harm the soundness of a country's financial sector. They can negatively affect the stability of individual banks or other financial institutions, such as securities firms and insurance companies. Criminal activity has been associated with a number of bank failures around the globe, including the closures of the first internet bank, European Union Bank, as well as Riggs Bank. The establishment and maintenance of an effective AML/CFT program is usually part of a financial institution's charter to operate; non-compliance can result not only in significant civil money penalties, but also in the loss of its charter.
- **Dampening Effect on Foreign Investments:** Although developing economies cannot afford to be too selective about the sources of capital they attract, there is a dampening effect on foreign direct investment when a country's commercial and financial sectors are perceived to be compromised and subject to the influence of organized crime. To maintain a business-friendly environment these impedances have to be weeded out.
- **Loss of Control of, or Mistakes in, Decisions Regarding Economic Policy:** Due to the large amounts of money involved in the money laundering process, in some emerging market countries these illicit proceeds may dwarf government budgets. This can result in the loss of control of economic policy by governments or in policy mistakes due to measurement errors in macroeconomic statistics.

  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. This is particularly true in economies based on the US dollar, as the tracking of monetary aggregates becomes more uncertain. Last, money laundering can increase the threat of monetary instability due to the misallocation of resources from artificial distortions in asset and commodity prices.
- **Economic Distortion and Instability:** Money launderers are not primarily interested in profit generation from their investments, but rather, in protecting their proceeds and hiding the illegal origin of the funds. Thus, they "invest" their money in activities that are not necessarily economically beneficial to the country where the funds are located. Furthermore, to the extent that money laundering and financial crime redirect funds from sound investments to low-quality investments that hide their origin, economic growth can suffer.
- **Loss of Tax Revenue:** Of the underlying forms of illegal activity, tax evasion is, perhaps, the one with the most obvious macroeconomic impact. Money laundering diminishes government tax revenue and, therefore, indirectly harms honest taxpayers. It also makes government tax collection more difficult. This loss of revenue generally means higher tax rates than would normally be the case.

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

- **Risks to Privatization Efforts:** Money laundering threatens the efforts of many states trying to introduce reforms into their economies through the privatization of state-owned properties such as land, resources, or enterprises. Sometimes linked with corruption or inside deals, a government may award a state privatization tender to a criminal organization potentially at an economic loss to the public. Moreover, 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 ports, resorts, casinos and other state properties to hide their illicit proceeds and to further their criminal activities.

- **Reputation Risk for the Country:** A reputation as a money laundering or terrorist financing haven can harm development and economic growth in a country. It diminishes legitimate global opportunities because foreign financial institutions find the extra scrutiny involved in working with institutions in money laundering havens is too expensive.

  Legitimate businesses located in money laundering havens may also suffer from reduced access to markets (or may have to pay more to have access) due to extra scrutiny of ownership and control systems. Once a country's financial reputation is damaged, reviving it is very difficult and requires significant resources to rectify a problem that could have been prevented with proper anti-money laundering controls. Other effects include specific counter-measures that can be taken by international organizations and other countries, and reduced eligibility for governmental assistance.

- **Risk of International Sanctions:** In order to protect the financial system from money laundering and terrorist financing, the United States, the United Nations, the European Union, and other governing bodies may impose sanctions against foreign countries, entities or individuals, terrorists and terrorist groups, drug traffickers, and other security threats. In the United States, the Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions.

  Countries can be subject to comprehensive or targeted sanctions. Comprehensive sanctions prohibit virtually all transactions with a specific country. Targeted sanctions prohibit transactions with specified industries, entities, or individuals listed on OFAC's Specially Designated Nationals and Blocked Parties List. Failure to comply may result in criminal and civil penalties. FATF also maintains a list of jurisdictions identified as high-risk and non-cooperative, whose AML/CFT regimes have strategic deficiencies and are not at international standards. As a result, FATF calls on its members to implement counter-measures against the jurisdiction such as financial institutions applying enhanced due diligence to business relationships and transactions with natural and legal persons from the identified jurisdiction in an attempt to persuade the jurisdiction to improve its AML/CFT regime.

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

  Financial institutions that rely on the proceeds of crime face great challenges in adequately managing their assets, liabilities and operations, attracting legitimate clients. They also risk being excluded from the international financial system. The adverse consequences of money laundering are reputational, operational, legal and concentration risks and include:

  — 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:** The potential that adverse publicity regarding an organization's business practices and associations, whether accurate or not, will cause a loss of public confidence in the integrity of the organization. As an example, reputational risk for a bank represents the potential that borrowers, depositors and investors might stop doing business with the bank because of a money laundering scandal.

  The loss of high-quality borrowers reduces profitable loans and increases the risk of the overall loan portfolio. Depositors may withdraw their funds. Moreover, funds placed on deposit with a bank may not be a reliable as a source of funding once depositors learn that the bank may not be stable. Depositors may be more willing to incur large penalties rather than leaving their funds in a questionable bank, resulting in unanticipated withdrawals, causing potential liquidity problems.

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

- **Legal Risk:** The potential for lawsuits, adverse judgments, unenforceable contracts, fines and penalties generating losses, increased expenses for an organization, or even the closure of the organization. For instance, legitimate customers may become victims of a financial crime, lose money and sue the financial institution for reimbursement. There may be investigations conducted by regulators and/or law enforcement authorities, resulting in increased costs, as well as fines and other penalties. Also, certain contracts may be unenforceable due to fraud on the part of the criminal customer.

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

For these reasons, international bodies have issued statements such as the Basel Committee on Banking Supervision's 2014 guidelines on the *Sound Management of Risks Related to Money Laundering and Financing of Terrorism* and *FATF's International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation.*

AML/CFT Compliance Programs and Individual Accountability

In the past several years, guidance has been issued and laws have been passed seeking individual accountability at the senior levels of regulated financial institutions that have contributed to deficiencies in AML and sanctions compliance programs.

In 2014, the Financial Crimes Enforcement Network (FinCEN) of the US Department of the Treasury and the U.S.' Financial Intelligence Unit (FIU) issued an advisory to financial institutions reminding them to maintain a strong culture of compliance and that the entire staff is responsible for AML/CFT compliance. This advisory was followed in 2015 by a memorandum on "Individual Accountability and Corporate Wrongdoing," from the US Department of Justice's Deputy Attorney General, Sally Quillian Yates.

The Yates Memo, as it is often referred to, reminds prosecutors that criminal and civil investigations into corporate misconduct should also focus on individuals who perpetrated the wrongdoing. Further, it notes that the resolution of a corporate case does not provide protection to individuals from criminal or civil liability. While the Yates Memo does not specifically address AML/CFT compliance, recent enforcement actions issued by US regulators against financial institutions illustrate a continued focus on AML/CFT compliance deficiencies.

In the United Kingdom, the Financial Conduct Authority (FCA) published final rules for the Senior Managers Regime (2015), which is designed to improve individual accountability within the banking sector. In relation to financial crime, the Senior Managers Regime requires a financial institution to give explicit responsibility to a senior manager, such as an executive=level Money Laundering Reporting Officer (MLRO), for ensuring that the institution's efforts to combat financial crime are effectively designed and implemented. The senior manager is personally accountable for any misconduct that falls within the institution's AML/CFT regime.

Finally, on June 30, 2016, the New York State Department of Financial Services (DFS) issued a Final Rule requiring regulated institutions to maintain "Transaction Monitoring and Filtering Programs" reasonably designed to:

(i) monitor transactions after their execution for compliance with the Bank Secrecy Act (BSA) and anti-money laundering (AML) laws and regulations, including suspicious activity reporting requirements; and

(ii) prevent unlawful transactions with targets of economic sanctions administered by the US Treasury Department's Office of Foreign Assets Control (OFAC).

This Final Rule, which goes into effect on January 1, 2017, also requires regulated institutions' boards of directors or senior officer(s) to make annual certifications to the DFS confirming that they have taken all steps necessary to comply with transaction monitoring and filtering program requirements.

While the law may seem New York-specific on its face, numerous foreign banks fall within the law because they operate in New York. Specifically, the law covers banks, trust companies, private bankers, savings banks, and savings and loan associations chartered pursuant to the New York Banking Law and all branches and agencies of foreign banking corporations licensed pursuant to the Banking Law to conduct banking operations in New York. Moreover, the law also applies to non-bank financial institutions with a Banking Law license such as check cashers and money transmitters.

Case Study

From 2003 to 2008, Thomas Haider served as the Chief Compliance Officer for MoneyGram, a money services business (MSB) specializing in money transfers. As part of his responsibilities, Mr. Haider was responsible for ensuring that MoneyGram had an effective AML/CFT program that requires timely reporting of suspicious transactions. He was also in charge of MoneyGram's Fraud Department.

During that time, there were thousands of complaints placed by customers who reported that they were victims of "lottery" or prepayment fraud and instructed to remit money to fraudsters via MoneyGram agents in the US and Canada. Although receiving a wealth of information from complainants Mr. Haider and MoneyGram's Fraud Department did not conduct an investigation of the complaints or the outlets from where the complaints were generated. An investigation would have allowed Mr. Haider to suspend or terminate any agent participating in the illegal activity.

According to a December 2014 FinCEN Assessment of Civil Penalty, Mr. Haider failed to implement an appropriate AML program, conduct effective audits, or terminate known high-risk agents. As a result of FinCEN's investigation, Mr. Haider was removed from his employment at MoneyGram in 2008 and was individually assessed a $1 million Civil Money Penalty in 2014. FinCEN also sought to bar Mr. Haider from working in the financial services industry.

Methods of Money Laundering

Money laundering is an ever-evolving activity; it must be continuously monitored in all its various forms in order for measures against it to be timely and effective. Illicit money can move through numerous different commercial channels, including products such as checking, savings and brokerage accounts, loans, wire and transfers, or through financial intermediaries such as trusts and company service providers, securities dealers, banks and money services businesses.

A money launderer will seek to operate in and around the financial system in a manner that best fits the execution of the scheme to launder funds. As many governments around the world have implemented AML obligations for the banking sector, a shift in laundering activity into the non-bank financial sector and to non-financial businesses and professions has risen.

FATF and FATF-style regional bodies publish periodic typology reports to "monitor changes and better understand the underlying mechanisms of money laundering and terrorist financing." The objective is to report on some of the "key methods and trends in these areas" and to also make certain that the FATF 40 Recommendations remain effective and relevant. In this chapter, we will refer often to these typologies because they give good examples of how money can be laundered through different methods and in different settings.

Banks and Other Depository Institutions

Banks have historically been and continue to be important mechanisms in all three stages of money laundering. Below are some special areas of interest and concern for money laundering through banks and other depository institutions.

ELECTRONIC TRANSFERS OF FUNDS

An electronic transfer of funds is any transfer of funds that is initiated by electronic means, such as an Automated Clearing House (ACH) computer, an automated teller machine (ATM), electronic terminals, mobile telephones, telephones or magnetic tapes. It can happen within a country or across borders, and trillions of dollars are transferred in millions of transactions each day as it is one of the fastest ways to move money.

Systems like the Federal Reserve Wire Network (Fedwire), the Society for Worldwide Interbank Financial Telecommunication (SWIFT) and the Clearing House Interbank Payments System (CHIPS) move millions of wires or transfer messages daily. As such, illicit fund transfers can be easily hidden among the millions of legitimate transfers that occur each day. For example, money launderers may initiate unauthorized domestic or international electronic transfers of funds — such as ACH debits or by making cash advances on a stolen credit card — and place the funds into an account established to receive the transfers. Another example is stealing credit cards and using the funds to purchase merchandise that can be resold to provide the criminal with cash.

Money launderers also use electronic transfers of funds in the second stage of the laundering process, the layering stage. The goal is to move the funds from one account to another, from one bank to another, and from one jurisdiction to another with each layer of transactions –making it more difficult for law enforcement and investigative agencies to trace the origin of the funds.

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

The processes in place to verify the electronic transfer of funds have been tightened in recent years. Many transaction monitoring software providers have sophisticated algorithms to help detect or trigger alerts that may indicate money laundering or other suspicious activity using electronic transfers of funds. However, no system is foolproof.

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

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

REMOTE DEPOSIT CAPTURE

Remote Deposit Capture (RDC) is a product offered by banks that allows customers to scan a check and transmit an electronic image to the bank for deposit. This offers increased convenience for customers as they no longer need to make a trip to the bank or an ATM to deposit checks. Previously, this was offered only via specialized scanners to commercial customers, but now many banks allow individuals to deposit pictures of checks taken with mobile phones. RDC decreases the cost to process checks for banks and is part of a gradual transition away from paper-based transactions. RDC is also increasingly used in correspondent banking for the same reasons, as it streamlines the deposit and clearing process. Correspondent banking is the provision of banking services by one bank to another bank.

The convenience provided by RDC leads itself to potential abuse by money launderers as he or she no longer needs to go into the bank and risk detection. Once a money launderer has RDC capabilities, he or she can move checks with ease through an account. It might even be possible to set up multiple imaging devices (e.g., multiple scanners and multiple permitted mobile phones) that will enable a money launderer to allow others to process checks through the system. It might even be possible for the money launderer to have someone else set up the account and provide him or her with the ability to deposit checks. Without proper controls, RDC can also be misused to facilitate violations of sanctions requirements (e.g., processing transactions in a sanctioned country).

While RDC can be used for money laundering, the more prominent risk relates to fraud. Since RDC minimizes human intervention in reviewing cleared items, the ability to identify potential fraud indicators, such as an altered check or multiple deposits of the same item, decreases. Often, the resulting fraud is not prevented but rather detected after it has already occurred.

To control the risks associated with RDC, efforts must be made to integrate RDC processing into other controls, such as monitoring and fraud prevention systems. In fact, this integration should occur with any new product offered by a bank. This includes ensuring that items submitted via RDC are reviewed for sequentially numbered checks and money orders without payees; that the total volume of activity processed for an account via RDC is incorporated into the overall transaction monitoring; that appropriate limits are placed on a customer's ability to deposit checks via RDC; that the product is offered to customers to whom it is appropriate; and that appropriate action is taken quickly when fraud is detected via RDC items.

CORRESPONDENT BANKING

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 services through correspondent relationships, including cash management (for example, interest bearing accounts in a variety of currencies), international wire transfers of funds, check clearing, payable-through accounts and foreign exchange services.

Before establishing correspondent accounts, banks should be able to answer basic questions about the respondent bank, including who its owners are and the nature of its regulatory oversight. Respondent banks judged to be sound credit risks may be offered a number of credit-related products (for example, letters of credit and business accounts for credit card transactions). The services offered by a correspondent bank to smaller, less well-known banks may be restricted to non-credit, cash management services.

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

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

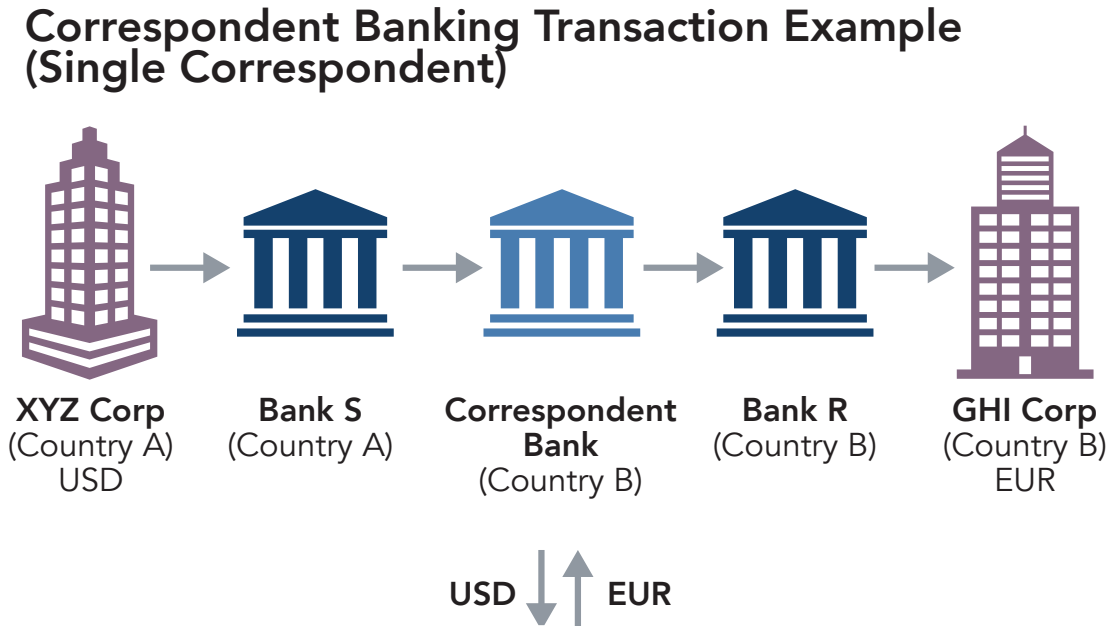
2. The amount of money that flows through correspondent accounts can pose a significant threat to financial institutions, as they process large volumes of transactions for their customers' customers. This makes it more difficult to identify suspect transactions, as the financial institution generally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

Additional risks incurred by the correspondent bank include:

- While the correspondent bank may be able to learn what laws govern the respondent bank, determining the degree and effectiveness of the supervisory regime to which the respondent is subject may be much more difficult. This can make it difficult to determine the level of risk associated with developing a relationship with a respondent bank.
- Determining the effectiveness of the respondent bank's AML controls can also be a challenge. While requesting compliance questionnaires will provide some comfort, the correspondent bank is still very reliant on the respondent doing its own due diligence on the customers it allows to use the correspondent account.
- Some banks offering correspondent facilities may not ask their respondents about the extent to which they offer such facilities to other institutions, a practice known as nesting. This means the correspondent bank is even further removed from knowing the identities or business activity of these sub-respondents, or even the types of financial services provided.

  Case Study

  In March 2015, US regulators closed Florida-based North Dade Community Development Federal Credit Union for willful violations of the USA PATRIOT Act, the Bank Secrecy Act (BSA), and provisions to its credit union charter and bylaws. The credit union had only one office staffed by five people. The credit union's purpose was to provide basic financial services to its members from the local community. However, FinCEN observed that the credit union had correspondent banking relationships with money services businesses (MSBs) in high-risk jurisdictions in Latin America and the Middle East. In 2013, the credit union processed approximately $55 million in cash orders, $1 billion in outgoing wire transfers, $5 million in returned checks, and $985 million in remote deposit capture for its MSB clients. FinCEN stated that these funds could have been linked to money laundering or supporting terrorist organizations. Moreover, FinCEN identified the activity was not expected business behavior of a small credit union like North Dade and led to substantial AML/CFT compliance failures and violations, including willfully violating its BSA program, record-keeping, reporting and requirements. As a result, North Dade consented to a $300,000 civil money penalty. Subsequently, the National Credit Union Association (NCUA), the banks' financial regulator, liquidated North Dade after determining it had violated various provisions of its charter, bylaws and federal regulations.



PAYABLE THROUGH ACCOUNTS

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

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

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

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

- PTAs with foreign institutions licensed in offshore financial service centers with weak or nascent bank supervision and licensing laws.

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

Case Study

Lombard Bank, a bank licensed by the South Pacific island of Vanuatu, opened a payable-through account at American Express Bank International (AEBI) in Miami. The Vanuatu bank was permitted to have multiple authorized signatures on the account.

Lombard customers had no relationship with AEBI. However, the bank offered its Central American customers virtually full banking services through its payable-through account at AEBI. They were even given checkbooks allowing them to deposit and withdraw funds from Lombard's payable-through account.

Lombard's PTA sub-account holders would bring cash deposits to Lombard representatives in four Central American countries. Lombard couriers would then 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 was also deposited in the payable-through account at AEBI. Over the two years ending in June 1993, as much as $200,000 in cash was received by Lombard's Miami affiliate on 104 occasions. As a result, AEBI lacked any visibility into the source of the cash being deposited by Lombard's customers' into the PTA at AEBI, raising significant AML/CFT compliance concerns with know your customer, due diligence, and record-keeping and regulatory filing requirements.

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. They do this by aggregating funds from several locations into one centralized account (i.e., the concentration account) and 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.

Money laundering risks can arise in concentration accounts if the customer-identifying information, such as name, transaction amount and account number, is separated from the financial transaction. If separation occurs, the audit trail is lost, and accounts may be misused or administered improperly.

Banks that use concentration accounts should implement adequate policies, procedures and processes covering operation and record-keeping for these accounts, including:

- Requiring dual signatures on general ledger tickets.

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

PRIVATE BANKING

Private banking is an extremely lucrative, competitive and global industry. Since the 2008 financial crisis, US and EU officials have placed greater scrutiny on private banks and their services, particularly in tax planning strategies.

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

Fierce competition among private bankers for the high net-worth individuals who are their main clientele has given rise to the need for tighter government controls worldwide. Competition brings increased pressures on the relationship managers and the marketing officers to obtain new clients, to increase their assets under management, and to contribute a greater percentage to the net income of their organizations. Plus, the compensation paid to most relationship managers in private banking is based largely on the assets under management that they bring to their institutions.

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

- Perceived high profitability.
- Intense competition.
- Powerful clientele.
- The high level of confidentiality associated with private banking.
- The close trust developed between relationship managers and their clients.
- Commission-based compensation for relationship managers.
- A culture of secrecy and discretion developed by the relationship managers for their clients.
- The relationship managers becoming client advocates to protect their clients.
- Use of private investment companies by clients to reduce transparency of the beneficial owner.
- Clients maintain personal and business wealth in numerous jurisdictions.

- Clients may utilize and control numerous legal entities for personal and family estate planning purposes

  Case Study

  Two private bankers formerly employed by American Express Bank International were convicted of money laundering for the Mexican drug cartel of Juan Garcia Abrego in 1994. For their role in the criminal activity, 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."

  Also in the United States, Riggs Bank maintained a close relationship with Augusto Pinochet, the former president of Chile. This relationship with Pinochet included flying to and from Chile on his private jet and taking hundreds of thousands of dollars' worth of cashier's checks to Pinochet. These funds were later found to be the proceeds of corruption. Riggs also facilitated the movement of money through real estate transactions that appeared to be structured in such a way as to avoid linking them to Pinochet. In May 2004, Riggs Bank, which was a well-respected bank founded in the 1800s, was fined $25 million for violations of the US Bank Secrecy Act. Subsequently, in 2005, Riggs pleaded guilty to a federal criminal violation of the Bank Secrecy Act repeated and systemic failure accurately to report suspicious monetary transactions associated with bank accounts owned and controlled by Augusto Pinochet of Chile and by the government of Equatorial Guinea. Riggs was fined $16 million, the largest criminal penalty ever imposed on a bank Riggs' size. As a result, Riggs also voluntarily closed its Embassy Banking and International Private Banking Divisions. Subsequently, Riggs was acquired by another bank and the Riggs name was retired.

USE OF PRIVATE INVESTMENT COMPANIES IN PRIVATE BANKING

In offshore or international financial centers, private banking customers are often "non-residents," meaning they conduct their banking in a country outside the one in which they reside. Their assets may move overseas where they are held in the name of corporate vehicles like private investment companies (PICs) established in secrecy havens. 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. They have been an element of many high-profile laundering cases in recent years as they are excellent laundering vehicles.

The secrecy laws of the offshore havens where PICs are often established can conceal the true identity of their beneficial owners. As an additional layer of secrecy, some PICs are established by company formation agents with nominee directors who hold title to the company for the benefit of individuals. These beneficial owners may remain undisclosed and sometimes subject to an attorney-client privilege or other similar legal safeguards. Many private banks establish PICs for their clients, often through an affiliated trust company in an offshore secrecy haven. Illicit actors may establish complex shell company networks where a company registered in one offshore jurisdiction may be linked to companies or accounts in other jurisdictions.

Case Study

In 2014 Israeli based institution, Bank Leumi Bank admitted that it assisted more than 1,500 US taxpayers in hiding their assets in Bank Leumi's offshore affiliates in Switzerland and Luxembourg. According to reports, for several years Bank Leumi sent private bankers to the US to meet with its US clients to discuss their offshore portfolio and tax mitigation strategies. As part of this, the bank assisted in organizing nominee corporate entities registered in Belize and other offshore jurisdictions to hide their clients' private offshore accounts, and maintained several US clients' accounts under assumed names or numbered accounts. Bank Leumi also provided "hold mail" services and offered loans to its US clients that were collateralized by their offshore assets that were not declared to US tax authorities. As a result of the settlement, Bank Leumi was assessed USD 270 million in fines and the bank was ordered to cease providing private banking and investment services for all US clients or accounts with US beneficial owners. This settlement led to Bank Leumi selling its affiliates Bank Leumi Private Bank and Bank Leumi (Luxembourg).

POLITICALLY EXPOSED PERSONS

According to FATF's International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (2012), there are two types of Politically Exposed Persons (PEPs):

- **Foreign PEPs:** Individuals who are or have been entrusted with prominent public functions by a foreign country, for example heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.
- **Domestic PEPs:** Individuals who are or have been entrusted domestically with prominent public functions, for example heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

PEPs have been the source of problems for several financial institutions, as the examples below show:

- **Mario Villanueva,** the corrupt governor of the Mexican state of Quintana Roo facilitated the smuggling of 200 tons of cocaine into the US, according to the US Drug Enforcement Agency (DEA). For five years, until 2001, he maintained private banking accounts at Lehman Brothers containing approximately $20 million that the DEA alleged he had received as bribes from Mexican drug traffickers.
- **The Riggs Bank** case revealed a web of transactions involving hundreds of millions of dollars that the bank had facilitated over many years for dictators on two continents, including **Augusto Pinochet** of Chile and **Teodoro Obiang** of Equatorial Guinea. The accounts formed part of the embassy banking portfolio that was the bank's specialty product for decades.
- **Vladimiro Montesinos,** the former head of Peru's Intelligence Service, and chief advisor of former Peruvian president Alberto Fujimori, had accounts at The Bank of New York in New York City, which held the proceeds from substantial bribes from drug traffickers. Other institutions, such as American Express Bank International, Bank of America, Barclays and UBS AG, in New

York, also held accounts for Montesinos. In addition, he used shell companies to facilitate embezzlement, gun running, drug trafficking, and money laundering in excess of $400 million globally.

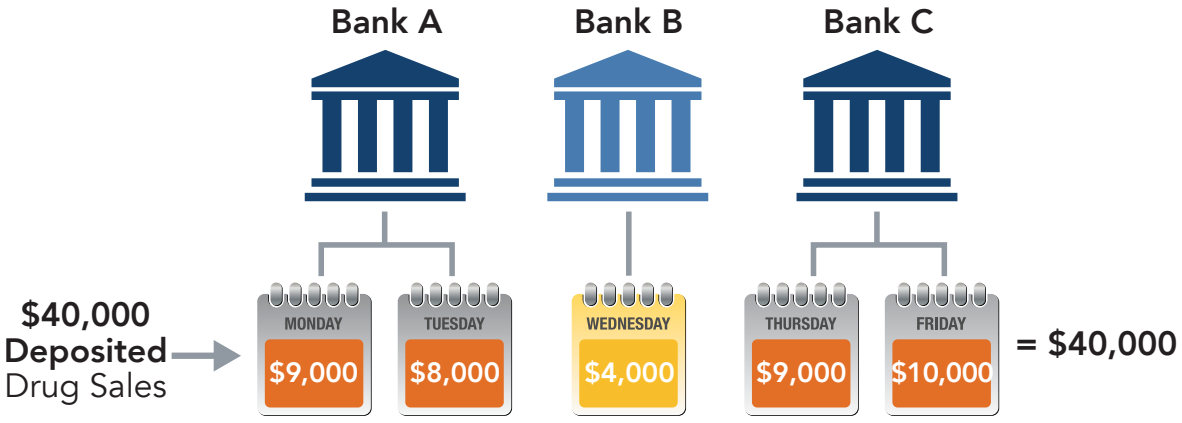
- **Arnoldo Aleman and Byron Jerez,** the former president and tax commissioner of Nicaragua, maintained accounts at Terrabank N.A. in Miami, through which they bought millions of dollars of certificates of deposit and condominiums in South Florida, allegedly with the proceeds of corruption.
- **Pavel Lazarenko,** the former prime minister of Ukraine, had accounts in San Francisco at Bank of America, Commercial Bank, Pacific Bank, WestAmerica Bank, and various securities firms, including Fleet Boston, Robertson & Stephens, Hambrecht & Quist and Merrill Lynch, where millions of dollars he allegedly extorted as head of state of Ukraine were held.
- **Colonel Victor Venero Garrido,** a Peruvian army officer, whom the US FBI described as the "most trusted bag/straw man" of Vladimiro Montesinos, maintained accounts at Citibank in Miami and Northern Trust in California that allegedly held more than $15 million in bribes and extortion proceeds.
- **Mario Ruiz Massieu,** the former deputy attorney general of Mexico in charge of drug trafficking prosecutions maintained a private banking account at Texas Commerce Bank in Houston in the mid-1990s, where he deposited drug traffickers' bribes of $9 million in currency over a 13-month period.
- **Omar Bongo,** the president of Gabon in Central Africa for 41 years until his death in 2009, used offshore shell companies to move over $100 million in suspected funds through private bank accounts, including providing large amounts of cash to family members for his benefit.

STRUCTURING

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

Structuring can be done in many settings or industries, including banking, money services businesses and casinos. A common technique involved in structuring is called 'smurfing,' which involves multiple individuals making multiple cash deposits and/ or buying multiple monetary instruments or bank drafts in amounts under the reporting threshold in an attempt to evade detection.

Cash Structuring Example



Structuring remains one of the most common reported forms of unusual activity. Below are some well-known examples:

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

  Henri wants to conduct a transaction involving $18,000 in cash. However, knowing that depositing it all at once would exceed the cash reporting threshold of $10,000 in cash and would trigger the filing of a currency transaction report, he goes to three different banks and deposits $6,000 in each.

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

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

- **A wealthy Chinese man send his fortune across to London**

  Mr. Lee sends his gained wealth of one million pounds in sums of $40,000 via friends and business contacts to a British bank in London. The reason why he is not sending it to his own bank account in London is that the Chinese government has currency controls in place for transaction over $50,000 abroad.

  Case Study

  Structuring has been around for a long time, as is evidenced by this case from the early 1980s. While the case is old, the method continues to be used: breaking down transactions below the reporting threshold.

  Isaac Kattan was a travel agent and businessman. Kattan allegedly laundered an estimated $500 million per year in drug money, all of it in cash. Couriers from a number of cities would visit him in his apartment, leaving boxes and suitcases full of money. The bagmen were messengers from narcotics distributors. The money was payment to their suppliers in Colombia. One of Kattan's

favorite places for making deposits was The Great American Bank of Dade County. Officials in the bank were bribed to accept his massive deposits without filing currency transaction reports (CTRs).

Hernan Botero allegedly had a similar but smaller operation to Kattan's. He laundered only about $100 million per year from cocaine deals out of his home near Palm Beach. Botero was indicted in the United States and testimony in federal court showed he had bribed officers and employees of the Landmark Bank in Plantation, Florida, to accept his deposits. The money was brought in to the bank almost daily by Botero front companies. From Landmark, the money was transferred to the Miami accounts of Colombian banks. From there, it was a simple matter to wire the money to banks in Colombia. Kattan and Botero were sentenced to 30-year terms in federal prison.

Here is how foreign money brokers structure transactions:

1. A structurer, who is acting for a foreign money broker, opens numerous checking accounts in Country A using real and fictitious names. Sometimes the structurer uses identification documents of dead people supplied by the money brokers.
2. With funds supplied by the money brokers, the structurer opens the accounts with inconspicuous amounts, usually in the low four-figures.
3. To allay bank suspicions, the money brokers sometimes deposit extra funds to cover living expenses and to give the accounts an air of legitimacy.
4. Once the accounts are opened, the structurer signs the newly issued checks, leaving the payee, date and amount lines blank.
5. He sends the signed blank checks to the money broker in country B, usually by courier.
6. A structurer may open as many as two dozen checking accounts in this fashion. It is not uncommon for brokers to have more than 20 of these checking accounts in Country A available at any given time.
7. 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.
8. The availability of hundreds of these accounts to Country B's money brokers leaves open the possibility that tens of millions of dollars may pass through them each year.

MICROSTRUCTURING

Another method of placing large amounts of illicit cash into the financial system is microstructuring. Microstructuring is essentially the same as structuring, except that it is done at a much smaller level. Instead of taking $18,000 and breaking it into two deposits to evade reporting requirements, the microstructurer breaks it into 20 deposits of approximately $900 each, making the suspicious activity extremely difficult to detect.

In the case of a Colombian drug cartel, the cash proceeds of US drug sales were deposited into accounts in New York with ATM cards linked to them. The cards were provided to associates in Colombia. Deposits were made on a regular schedule with the Colombian associates withdrawing the funds as they were deposited and providing them to the drug lords. In one case in New York, an individual was trailed by law enforcement authorities as he went from bank to bank in Manhattan. When they stopped him, he had $165,000 in cash.

Methods of detecting microstructuring include:

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

Credit Unions and Building Societies

Credit unions, also known as building societies in some jurisdictions, are not-for-profit, member-owned and -operated democratic financial co-operatives.

Credit unions do not have clients or customers; instead they have members who are also owners. Credit unions serve only the financial needs of their members, and are governed by a "one member, one vote" philosophy. A member must purchase an initial capital share of the credit union, permitting him or her to access the products and services offered by the credit union. Credit union membership is based on a common bond, a linkage shared by savers and borrowers who belong to a specific community, organization, religion or place of employment.

Credit unions may vary greatly in both size and complexity. Some credit unions may have a few hundred members while others may have hundreds of thousands of members with tens of billions of dollars in assets under management. Some credit unions will focus on meeting only a few niche needs of their members, while others will offer a full suite of products and services to rival most retail banks.

Most credit unions focus primarily on servicing personal banking relationships from within their community. Depending on their member eligibility model, some may also facilitate memberships for small to medium-sized corporate and entity account holders, though the credit union may be prohibited from doing so in certain jurisdictions. Generally, credit unions do not participate in trade-based financing, will not facilitate correspondent banking relationships, and will not maintain large corporate relationships, particularly those with international banking needs.

In many jurisdictions, credit unions rely on credit union centrals for a variety of services. A credit union central is best defined as a trade association for credit unions; it is owned by its member credit unions and helps to serve many of their financial needs. Services may include those related to capital liquidity; research, training, and advocacy with respect to regulatory obligations; shared operational or back-office processes like check clearing and electronic funds transfer (EFT) processing. In general, they help to negotiate shared contracts for common services allowing many smaller credit unions to leverage economies of scale that they would not otherwise be able to do.

With respect to regulatory requirements and oversight, credit unions operate very similarly to banks in most jurisdictions. They have similar capital, liquidity, risk management, record-keeping, and reporting obligations as banks, though there may be some minor differences between institutions that are subject to the oversight of regional versus federal regulators and regulations. As credit unions are included under FATF's definition of a "financial institution," national AML/CFT regimes that follow FATF's recommendations treat credit unions similarly to banks.

The United Kingdom's Joint Money Laundering Steering Group (JMLSG) stated in its November 2006 guidance that, although credit unions pose a low money laundering risk due to their smaller average size and fewer products offered, they are still vulnerable to money laundering and terrorist financing schemes. Not surprisingly, the JMLSG found that the more financial services a credit union offers, the higher the potential risk for money laundering, as these credit unions or building societies tend to contain a larger clientele and offer potential criminals a larger range of possible ways to conceal their illicit funds.

In November 2014 guidance by the JMLSG, the group concluded that high-risk transactions include: money transfers to third parties, third parties paying in cash for someone else, and reluctance to provide identity information when opening an account. And as credit unions typically deal with small amounts and members with very regular behavior, another money laundering indicator given in the guidelines is there are transactions of larger than usual amounts and erratic member behavior.

The JMLSG even advised credit unions to watch for unusual activity in the accounts of children because parents could be trying to use those funds for illicit purposes, thinking such transactions would draw less attention. Examples in the past have shown that even bankrupted companies continued their operations on the bank accounts of children.

Non-Bank Financial Institutions

CREDIT CARD INDUSTRY

The credit card industry includes:

- Credit card associations, such as American Express, MasterCard and Visa, which license member banks to issue bankcards, authorize merchants to accept those cards, or both
- Issuing banks, which solicit potential customers and issue the credit cards.
- Acquiring banks, which process transactions for merchants who accept credit cards.

- Third-party payment processors (TPPP), which contract with issuing or acquiring banks to provide payment processing services to merchants and other business entities, typically initiating transactions on behalf of merchant clients that do not have a direct relationship with the TPPPs financial institution.

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

Example

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

A money launderer places his ill-gotten funds in accounts at offshore banks and then accesses these funds using credit and debit cards associated with the offshore account. Alternatively, he smuggles the cash out of one country into an offshore jurisdiction with lax regulatory oversight, places the cash in offshore banks and accesses the illicit funds using credit or debit cards.

In a 2002 report called, "Extent of Money Laundering through Credit Cards Is Unknown," the US Government Accountability Office, the Congressional watchdog of the United States, offered the following hypothetical money laundering scenario using credit cards: "Money launderers establish a legitimate business in the US as a 'front' for their illicit activity. They establish a bank account with a US-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 US-based bank has affiliates, they make withdrawals from their US bank account, using credit cards and ATM cards. Money is deposited by one of their cohorts in the US and is transferred to pay off the credit card loan or even prepay the credit card. The bank's online services make it possible to transfer funds between checking and credit card accounts."

THIRD-PARTY PAYMENT PROCESSORS

Third-party payment processors are generally bank customers that provide payment-processing services to merchants and other business entities and often use their commercial bank accounts to conduct payment processing for their merchant clients. Oftentimes, they are not subject to any AML/CFT requirements.

TPPPs traditionally contracted with US retailers (i.e., merchants) that had physical locations in the United States in order to help collect monies owed by customers. These merchant transactions primarily included credit card payments, but also covered Automated Clearing House (ACH) debits and creating and depositing remotely created checks (RCCs) or demand drafts. With the expansion of the internet, TPPPs may now service a variety of domestic and international merchants, including conventional retail and internet-based establishments as well as prepaid travel and internet gaming

enterprises. Considering the expansion of services and the fact that a financial institution maintains a relationship with the TPPP and not the underlying merchant, it becomes difficult for the financial institution to know on whose behalf it is processing a transaction.

The types of merchants that a TPPP provides its payment processing services to can increase the TPPP's vulnerability to money laundering, identity theft, fraud, and other illegal activity. For example, TPPPs that provide services to telemarketing, gambling (online, casinos, etc.), or internet merchants and/or process RCCs for these entities may present a higher level risk of risk to a financial institution, as these types of businesses carry a high risk for consumer fraud and money laundering.

Examples of risks posed by TPPP include:

- **Multiple Financial Institution Relationships:** The TPPP may maintain relationships at multiple institutions, which hinders a financial institution's ability to see the entire customer relationship. This is done on purpose by TPPPs engaged in suspicious activity to limit the financial institutions' ability to recognize suspicious activity and exit the relationship.
- **Money Laundering:** TPPPs can be used by criminals to mask transactions and launder the proceeds of crime. One way to engage in money laundering through a TPPP is to send funds directly to a financial institution from a foreign jurisdiction through an international ACH payment. Given the large number of transactions conducted through a TPPP, this activity may not be identified.
- **High Return Rates from Unauthorized Transactions:** TPPPs engaged in suspicious activity or being used by criminals may have higher than average return rates related to unauthorized transactions. At the merchant level, the criminal merchant may have acceptable return rates compared to the percentage of the TPPP's total transaction volume, but when compared against individual originators, the return rate will be significantly higher.

It is important to understand that credit card transactions, whether conducted through a TPPP or other financial institution do not have to be significant to be considered 'suspicious' or 'unusual.' For example, there may be a large number of small dollar transactions, repeat customers or donors with no discernible pattern, and/or receiving international donations or other payments that do not match with information provided by the customer when they described their business or based on historical activity conducted by the customer. Therefore, it is important to have strong customer and enhanced due diligence and transaction monitoring controls to detect suspicious activity and customers you do not want to do business with.

MONEY SERVICES BUSINESSES

A money services business (MSB), or money or value transfer service (MVTS) as defined by FATF, transmits or converts currencies. Such businesses usually provide currency exchange, money transmission, check-cashing, and money order services.

MSB laws vary by jurisdiction. For example, in the United States, FinCEN defines MSB to include any person doing business, whether or not on a regular basis or as an organized business concern, in one or more of the following capacities:

- **Dealer in Foreign Exchange:** These MSBs provide currency exchange services (e.g., USD converted to Euro). They typically operate along international borders, airports, or near communities with high populations of foreign individuals.
- **Check Casher:** Check-cashing services may be offered by retail businesses or as a stand-alone operation. Depending on the model, the MSB may cash checks for consumers and/or commercial businesses. In addition to check cashing, these MSBs may also provide other financial services so their customers can pay bills, purchase money orders or transmit funds domestically or internationally.
- **Issuer of Traveler's Checks or Money Orders:** The issuer of a money order or traveler's check is responsible for the payment of the item and often uses agents to sell the negotiable items.
- **Money Transmitter:** — Money transmitters accept currency or funds for the purpose of transferring those funds electronically through a financial agency, institution or electronic funds transfer network. Examples of well-known money transmitters are Western Union, MoneyGram, and PayPal.
- **Provider and Seller of Prepaid Access:** Providers of prepaid access arrange for access to funds or to the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number, or personal identification number. Sometimes prepaid access can also be referred to as stored value. Prepaid access can be open loop or closed loop:
  - — **Open loop prepaid cards** can be used for purchases at any merchant that accepts cards issued for use on the payment network associated with the card and to access cash at any ATM that connects to the affiliated ATM network. Examples of open loop prepaid access usually are branded with the network logo such as American Express, Visa, MasterCard.
  - — **Closed loop prepaid card**s are typically limited to buying goods or services from the merchant issuing the card. Sellers of prepaid access are those who exceed a certain threshold of prepaid access to one individual on a given day.
- **US Postal Service:** Since the US Postal Service sells its own money orders, it is deemed to be an MSB.

FinCEN published a Final Rule in 2012 to expand the MSB definition to detail when an entity qualifies as an MSB based on its activities within the United States, even if none of its agents, agencies, branches or offices are physically located there. The Final Rule arose in part from the recognition that the internet and other technological advances make it increasingly possible for persons to offer MSB services in the United States from foreign locations. Absent an exception, MSBs are required to register with FinCEN.

As another example, MSBs in Canada are defined as businesses engaged in foreign exchange dealing, money transferring, or cashing or selling money orders, traveler's checks and similar monetary instruments to the public. They are required to register with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

An MSB's business model can range from small, independent business to large multinational organizations. Organizations can either provide MSB services as their primary business or as ancillary service to primary retail store operations. Businesses that provide ancillary MSB services typically include grocery stores, drug stores, restaurants and bars. The services provided by these businesses include but are not limited to cashing payroll checks and selling prepaid cards. While many of these businesses have brick-and-mortar locations, MSBs operating solely on the internet with no physical presence or a network of agents are increasing.

Traditional MSBs typically provide services to the underserved or un-banked individuals. The focus on this market may put their operations in regions with limited or no banking services. Additionally, they typically provide lower cost services compared to financial institutions for certain service offerings. For example, engaging in domestic or international wire transfers through a financial institution can be time consuming and costly for a consumer. Conducting similar transactions through an MSB can happen quickly and at a much lower cost. Additional services can include bill payments, payday lending, and commercial check cashing.

MSBs can be categorized into principals or agents. Principals primarily provide MSB services and act as the issuers of money orders and traveler's checks or the providers of money transmission. In the United States, principal MSBs are required to have written AML policies, procedures, and internal controls; appoint a Bank Secrecy Act (BSA) Officer, provide education and training, conduct independent reviews/audits, and monitor transactions for suspicious activity.

Agents are entities seeking to provide MSB-type services in addition to its existing products and services. An agent may be a principal MSB in that it offers check cashing as its primary service, but an agent in that it provides money transmission services through a principal money transmitter MSB. For the agent to use such money transmission services, they must enter into an agent service agreement with a principal MSB. An additional byproduct of the principal/agent relationship is that it allows principal MSBs to expand their business and reach a wider customer market without the need for added overhead. As an agent of a principal MSB, the agent is required to follow the same state and federal regulations as a principal MSB (e.g., AML procedures and suspicious activity monitoring).

Examples of how MSBs can be used by criminals:

- Fraud in the healthcare industry has grown dramatically in recent years. Healthcare businesses, such as home healthcare businesses, engaged in fraudulent practices will present checks derived from fraud to check cashers who they know will not ask for proof of the payee's identity, will either not file or file false currency transaction reports (CTRs), and not report them to the government for engaging in suspicious activity. The check casher may be compromised by an employee insider or is attempting to be business friendly by avoiding complying with legal or regulatory requirements that are seen are burdens to its customers.
- Criminals obtain low cost workers' compensation insurance policies by grossly deflating payroll amounts. After securing certificates of insurance, organizers 'rent' the certificates to other individuals and businesses for a fee. Since the policies are obtained fraudulently, employees are not covered and therefore left vulnerable to high-dollar medical costs in the event of an

on-the-job injury. The payroll amounts are then concealed by cashing checks at an MSB, which circumvents proper bookkeeping measures. The criminal makes a significant amount of money at the detriment of workers.

- Money launderers use money remitters and currency exchanges 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.

  Case Study

  This is an example of money laundering utilizing MSBs from FINTRAC's Money Laundering Typologies and Trends for Canadian MSBs report.

  Two individuals were suspected of running a mass marketing fraud (MMF) scheme. The perpetrators used MSBs to receive payments from fraud victims in the United States. Counterfeit checks were sent to US residents, who were then instructed to send a portion of these funds back to two individuals perpetrating the fraud.

  One of the individuals, who appeared to use two identities and various addresses, was the beneficiary of most of the electronic funds transfers (EFTs) sent through the MSBs. He (or she) regularly received EFTs from US-based fraud victims over a short period of time. Since nearly all of the EFT amounts were below mandatory threshold amounts, it is possible that many more EFTs were sent to the suspected fraud perpetrator before suspicions were triggered regarding the financial activity. Over the course of a year, in excess of three dozen suspicious transaction reports (STRs) were filed on this individual.

  The other individual shared the same residential address with the first suspect, although the address was apparently never used when receiving the EFTs. He (or she) was thought to be the mastermind of the scheme as he had been convicted of a large number of fraud-related offenses. He had been flagged in reports sent to the government for a series of multiple cash deposits and in relation to depositing MSB-issued checks. The same individual also received Euro-denominated EFTs from Europe.

  The main EFT recipient (who used two identities and eight addresses) appeared to be using multiple MSB agents (close to twenty locations) in an attempt to conceal the fraudulent activity. Funds were paid out in checks issued by the MSB. STRs filed by a bank indicate that this individual made a series of deposits into two different banks accounts using cash and checks.

The biggest misconception about the MSB industry is that there is minimal oversight. In fact, many MSBs are overseen by a variety of national and/or local regulators and often maintain compliant AML programs. In addition, they are monitored by the banks that they maintain relationships with. However, the scrutiny to which MSBs are subject can vary greatly, in large part due to the ease with which some MSBs can set up business. Additionally, many MSBs are small (i.e., one-store operators) and may not have robust AML programs compared to their larger, national counterparts. This is why one of the most important aspects of due diligence for a bank when establishing a relationship with an MSB is to confirm that the MSB has implemented a sufficient AML program (e.g., procedures, training, and suspicious activity monitoring), and is properly licensed and/or registered in the jurisdictions they operate in.

INSURANCE COMPANIES

The insurance industry provides risk transfer, savings and investment products to a variety of consumers worldwide, ranging from individuals to large corporations to governments. An important aspect of the way the insurance industry operates is that most of the business conducted by insurance companies is transacted through intermediaries such as agents or independent brokers. Insurers, with some exceptions, are subject to AML requirements.

The susceptibility of the insurance industry to money laundering is not as high in comparison to other types of financial institutions. For example, 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. That said, certain sectors of the insurance industry, such as life insurance and annuities, are a primary target of criminals engaging in money laundering and/or terrorist financing. In a number of ways, the sector's vulnerability to money laundering is similar to that of the securities sector; in some jurisdictions, life insurance policies are even viewed as investment vehicles similar to securities.

According to FATF in its 2004-2005 typologies report, across the whole insurance sector, life insurance appears to be by far the area most attractive to money launderers. Substantial sums can be invested in widely available life insurance products and many feature a high degree of flexibility, whilst at the same time ensuring non-negligible rates of return. Many life insurance policies are structured to pay a fixed dollar amount upon death of the insured party while other life insurance products, such as whole or permanent life insurance, have an investment value, which can create a cash value above the original investment if it is canceled by the policy holder. Such characteristics, whilst of considerable value to the honest policyholder, also offer money launderers various opportunities to legitimize their ill-gotten funds. Furthermore, the most frequently observed individual typology relates to international transactions, which is evidence of the cross-border reach of insurance-related money laundering operations.

For criminals looking to launder funds, life insurance products with no cash surrender value are the least attractive. Those that feature payments of cash surrender value and the opportunity to nominate beneficiaries from the first day of the policy are the most attractive.

Annuities are another type of insurance policy with cash value. An annuity is an investment that provides a defined series of payments in the future in exchange for an up-front sum of money.

Annuity contracts may allow criminals to exchange illicit funds for an immediate or deferred income stream, which usually arrives in the form of monthly payments starting on a specified date. In both cases, a policyholder can place a large sum of money into a policy with the expectation that it will grow based on the underlying investment, which can be fixed or variable. One indicator of possible money laundering is when a potential policyholder is more interested in a policy's cancellation terms than its benefits.

Vulnerabilities in the insurance sector include:

- **Lack of oversight/controls over intermediaries:** Insurance brokers have a great deal of control and freedom regarding policies.

- **Decentralized oversight over aspects of the sales force:** Insurance companies may have employees (i.e., captive agents) who are subject to the full control of the insurance company. Non-captive agents offer an insurance company's products, but are not employed by an insurance company. They often work with several insurance companies to find the best mix of products for their clients and may fall between the cracks of multiple insurance companies. Some may work to find the company with the weakest AML oversight if they are complicit with the money launderer.
- **Sales-driven objectives:** The focus of brokers is on selling the insurance products and, thus, they often overlook signs of money laundering, such as a lack of explanation for wealth or unusual methods for paying insurance premiums.

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

- Certain insurance policies operate in the same manner as unit trusts or mutual funds. The customer can over-fund the policy and move funds into and out of the policy while paying early withdrawal penalties. When such funds are reimbursed by the insurance company (by check, for example), the launderer has successfully obscured the link between the crime and the generated funds.
- The purchase and redemption of single premium insurance bonds are key laundering vehicles. The bonds can be purchased from insurance companies and then redeemed prior to their full term at a discount. In such cases, the balance of the bond is paid to a launderer in the form of a "sanitized" check from the insurance company.
- A free-look period is a feature that allows investors — for a short period of time after the policy is signed and the premium paid — to back out of a policy without penalty. This process allows the money launderer to get an insurance check, which represents cleaned funds. However, as more insurance companies are subject to AML program requirements, this type of money laundering is more readily detected and reported.
- One indicator of possible money laundering is when a potential policyholder is more interested in the cancellation terms of a policy than the benefits of the policy. The launderer buys a policy with illicit money and then tells the insurance company that he has changed his mind and does not need the policy. After paying a penalty, the launderer redeems the policy and receives a clean check from a respected insurer.

The 2004-2005 FATF Money Laundering Typologies report provides some additional typologies related to the insurance industry:

- The funding of insurance policies by third parties (i.e., not the policyholder) who have not been subject to regular identification procedures when the insurance contract was concluded. The source of funds and the relationship between policyholder and third party is unclear to the insurance company.
- The customer actually does not seek insurance coverage but an investment opportunity. Money laundering is enabled by using large sums of money to make substantial payments into life insurance single premium policies, which serve as a wrapped investment policy. A variation on this is the use of large premium deposits used to fund annual premiums. Such policies, which are comparable to single premium policies, again enable the customer to invest substantial amounts

of money with an insurance company. Since the annual premiums are paid from an account that has to be funded with the total amount, an apparently lower money-laundering risk life product will bear the features of the higher risk single premium policy.

In the insurance sector most of the business is conducted through intermediaries. As a result, on most occasions it is intermediaries' application of the AML regulatory requirements that is unsatisfactory.

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 securities industry provides opportunities for criminals to engage in money laundering and terrorist financing anonymously, given the varying levels of AML program requirements in different types of businesses and the high volume of transactions. The world capital markets are vast in size, dwarfing deposit banking. According to the World Bank, in 2015 the market capitalization of listed companies alone totaled over US$61.7 trillion.

FATF has urged money laundering controls for the securities field since 1992, in conjunction with the Montreal-based International Organization of Securities Commissions (IOSCO), a global association of governmental bodies that includes the Commodity Futures Trading Commission (CFTC), which regulates the securities and futures markets. The difficulty in dealing with laundering in the securities field is that, usually, little currency is involved. It is an industry that runs by electronic transfers and paper. Its use in the money laundering process is generally after launderers have placed their cash in the financial system through other methods.

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

- Its international nature.
- The speed of the transactions.
- The ease of conversion of holdings to cash without significant loss of principal.
- The routine use of wire transfers to, from and through multiple jurisdictions.
- The competitive, commission-driven environment, which, like private banking, provides ample incentive to disregard the source of client funds.
- The practice of brokerage firms of maintaining securities accounts as nominees or trustees, thus permitting concealment of the identities of the true beneficiaries.
- Weak AML programs that do not have effective customer due diligence (CDD), suspicious activity monitoring, or other controls.

The illicit money laundered through the securities sector can be generated by illegal activities both from outside and from within the sector. For illegal funds originating outside the sector, securities transactions for the creation of legal entities may be used to conceal or obscure the source of these funds (i.e., layering). In the case of illegal activities within the securities market itself — for example embezzlement, insider trading, securities fraud, and 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.

Money laundering can occur in the securities industry in customer accounts that are used only to hold funds and not for trading. This allows launderers to avoid banking channels where the launderer may believe there are more stringent money laundering controls. Other indications of money laundering are "wash trading" or offsetting transactions. This involves the entry of matching buys and sells in particular securities, which creates the illusion of trading. Wash trading through multiple accounts generates offsetting profits and losses and transfers of positions between accounts that do not appear to be commonly controlled.

The 2009 FATF Money Laundering and Terrorist Financing in the Securities Sector typologies report identified the following areas as presenting the greatest money laundering vulnerabilities:

- Wholesale markets
- Unregulated funds
- Wealth management
- Investment funds
- Bearer securities
- Bills of exchange

Several challenges that are unique to the securities sector include:

• Variety and complexity of securities

Security offerings are broad with some products tailored to the needs of a single customer while others are designed for sale to the general public. Products range from the simple and almost universally known to the relatively complex and esoteric. Some knowledge of the underlying security is typically required in addressing risk.

• High-risk securities

While most securities are issued by legitimate companies, there are risks posed by securities that are under-regulated or established for illegitimate purposes. In the United States, securities that are not traded on regulated exchanges are typically sold over-the-counter, with tiers such as "pink sheets" that require only minimal reporting, thus making it easy to obscure information such as beneficial owners. This can make it difficult to determine associations with sanctioned jurisdictions or companies. Securities firms are required to not only identify securities that may cause risks but also develop processes to restrict trading of those securities, often on dozens of platforms.

- **Multiple layers and third-party risk**

The securities industry has many participants, including financial institutions and broker-dealers, financial advisors, transfer agents, securities lenders, custodians, introducing brokers and sales agents. The many layers of intermediaries, who may also cross borders, make standardizing controls difficult and further challenge overall compliance.

FATF has identified a number of suspicious indicators within the global securities markets. Those particularly relevant to the securities sector include:

- A customer with a significant history with the securities firm who abruptly liquidates all of his or her assets in order to remove wealth from the jurisdiction.
- A customer who opens an account or purchases a product without regard to loss, commissions or other costs associated with that account or product, including with early cancellations of long-term securities.
- The securities account is used for payments or outgoing wires with little or no securities activities (e.g., account appears to be used as a depository account or a conduit for transfers).
- A customer's transactions include a pattern of sustained losses. This may be indicative of transferring value from one party to another.
- Transactions where one party purchases securities at a high price and then sells them at a considerable loss to another party. This may be indicative of transferring value from one party to another.
- A customer who is unfamiliar with a financial product's performance and specifications but wants to invest in it nonetheless.
- A customer who is known to have friends or family who work for the securities issuer or a trading pattern suggests that he or she may have nonpublic information.
- Two or more unrelated accounts at a securities firm trade an illiquid or low-priced security (penny stock) suddenly and simultaneously.
- A customer who deposits physical securities that are: 1) in large quantities, 2) titled differently from the name of the account, 3) do not bear a restrictive legend even though the history suggests that it should, or 4) the method of acquiring the securities lacks sense.

  Case Study

  In June 2016, Albert Fried & Co. (AFCO), a US registered broker-dealer, settled charges with the SEC for failing to monitor a customer's trades for suspicious activity as required under federal securities laws. Customer A deposited with and sold through AFCO more than 119 million shares of four penny stocks over a four-month period. On one day, the customer's trades represented over 85 percent of the daily volume in a single stock and on numerous other days the trading accounted for over 50 percent.

  Numerous red flags should have raised concerns for AFCO and prompted further investigation or reporting, such as: 1) the stock issuers were the subject of promotional campaigns at the time of the customer's trading, 2) the broker-dealer was aware that the issuer underwent a 5:1 reverse

stock split shortly after Customer A deposited that issuer's securities into its AFCO account, 3) the broker-dealer received numerous regulatory and criminal inquiries regarding Customer A's trading in at least three securities, and 4) the Commission suspended trading in an issuer's stock only three months after Customer A sold large volumes of the issuer's securities.

Broker-dealers have a duty to detect red flags and perform additional due diligence, especially when the indicators are related to penny stock transactions. The use of broker-dealers by criminals to launder proceeds of crime or conduct fraud is common throughout the industry. Canada's FINTRAC provides a good case study of such a scheme:

Case Study

A group of individuals who were suspected of manipulating the share price of Company X, which traded over-the-counter in the United States, in what is commonly referred to as a "pump and dump" scheme. Individual 1 purchased shares in the company at a low price. Typical of the "pump" aspect of these types of schemes, the group produced fraudulent reports on the company's prospects that caused the shares to increase sharply in value. According to law enforcement, the perpetrators of the scheme approached an organized crime group to launder the criminal proceeds that resulted from the sale of shares following the artificial price inflation.

Individual 2 deposited physical share certificates of Company X into a brokerage account. Individual 2 was suspected of being a nominee for the organized crime group. Shortly after the deposits of the physical share certificates, Individual 2 engaged in what appeared to be a structured sale of the shares, characteristic of the "dump" phase of this type of fraud. Following the sale of the shares, Individual 2 requested early settlement in the form of certified checks.

The certified checks were deposited into Individual 2's bank account held at a financial institution that was not affiliated with the brokerage firm. Individual 2 ordered multiple EFTs to a company located in Central America, the beneficial owner of which was Individual 1.

Retail broker-dealers are the industry's frontline defense — and its most vulnerable access point. They are under constant management pressure to expand their client base and to manage more assets. The more assets in a client's account, the more commission will be generated. A money launderer can potentially use this to his advantage by promising a large or steady commission stream. As such, it is important for broker-dealers to understand who they are doing business with and to monitor for suspicious activity.

In the United States, the SEC and the Financial Industry Regulatory Authority (FINRA), as directed by the Bank Secrecy Act (BSA) regulatory rules, have implemented requirements for broker-dealers at both small and large firms to implement AML programs that include: an appointed BSA Officer, performing CDD, suspicious activity monitoring, training and an independent audit. These requirements also subject broker-dealers to oversight by either the SEC, FINRA, or both to monitor if and how they are complying with the AML program requirements. Lack of, or weak, AML program requirements can lead to substantial monetary and criminal penalties.

Non-Financial Businesses and Professions

CASINOS

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

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

Money laundering through casinos generally occurs in the placement and layering stage (for example, converting the funds to be laundered from cash to checks and utilizing casino credit to add a layer of transactions before the funds are ultimately transferred out). A launderer can buy chips with cash generated from a crime and then request repayment by a check drawn on the casino's account. Often, rather than requesting repayment by check in the casino where the chips were purchased with cash, the gambler says that he will be traveling to another country in which the casino chain has an establishment, asks for his credit to be made available there and withdraws it in the form of a check in the other jurisdiction. Money launderers can also establish a casino line of credit and use illegitimately obtained funds as a repayment on the credit line.

In its 1997-1998 typologies report, FATF reported that gaming businesses and lotteries were being used increasingly by launderers. FATF gave examples of gambling transactions that enabled drug dealers to launder their money through casinos and other gambling establishments. One laundering technique connected with horse-racing and gaming is when the person will actually gamble the money to be laundered, but in such a way as to be reasonably sure of ultimately recovering his stake in the form of checks issued or funds transfers by the gambling or betting agency and reflecting verifiable winnings from gaming. This method makes it more difficult to prove the money laundering because the person has actually received proceeds from gambling.

Junkets, a form of casino-based tourism, also present significant money laundering risk as junket participants largely rely on third parties, junket operators, to move the funds across borders and through multiple casinos, creating layers of obscurity around the source of funds and ownership of the money and the identities of the players. In some jurisdictions, casinos may enter into a contractual agreement with a junket operator to rent a private gaming room, and in some situations is it the junket operator, not the casino, that monitors player activity and issues and collects credit. Additionally, some jurisdictions allow junket operators to pool funds, which obscures the spending of individual customers. In certain regions, licensed junket operators act as fronts for junket operators in another country. The front operators supply players to a casino through a casino's licensed junket companies, which may not qualify for a license in the country where the players will be

gambling. Such unlicensed sub-junket operators can act as unlicensed collectors of credit and may have ties to organized crime networks. This poses serious risk, and can lead a casino to engage in informal arrangements with junket operators that are inconsistent with AML/CFT policies.

In its 2009 Report, FATF recognized that a number of jurisdictions do not require licensing of junket operators and their agents, further increasing the risks described above, and stressed the need to ensure that junket operators are not under criminal influence and to ensure that financial transactions are transparent and subject to relevant AML/CFT measures.

FinCEN's 2008 Guidance and FATF's 2009 Report on Casinos and Gaming Sector identified specific behaviors to watch for:

- Attempts to evade AML reporting or record-keeping requirements, such as:
  - A customer pays off a large credit debt, such as markers or bad checks, over a short period of time through a series of currency transactions, none of which exceeds the reportable threshold.
  - Two or more customers each purchase chips in small amounts, engage in minimal gaming, then combine the funds to request a casino check for the chips presented.
  - A customer receives a large payout in excess of $10,000 but requests currency of less than $10,000 and the balance paid in chips. He then goes to the cage and redeems the remaining chips in the amounts less than the reporting threshold.
  - A customer structures the transaction, by often involving another customer, to avoid filing of the CTR or another tax form.
  - A customer reduces the amount of chips presented for a cash-out when asked for ID to stay under the reportable threshold.
- Using the cage solely for its banking-like financial services, such as:
  - A customer wires funds derived from non-gaming proceeds, to or through a bank/non-bank financial institution located in a country that is not his residence or place of business.
  - A customer appears to use a casino as a temporary repository for funds by making frequent deposits into the casino account and, within a short period of time, requests money transfers to domestic or foreign-based bank account.
- Minimal gaming activity without a reasonable explanation, such as:
  - A customer purchases a large amount of chips, engages in minimal gaming, and then redeems the chips for a casino check.
  - A customer uses an established casino credit line to purchase chips, engages in minimal play, then pays off the credit in currency and redeems the chips for a casino check.
  - A customer makes a large deposit using small denomination bills and withdraws it in chips at the table; engages in minimal play, then exchanges the chips at the cage for large denomination bills.

— A customer inserts large amounts of small denominations bills into a slot machine ("bill-stuffing"), engages in minimal or no play, and exchanges the voucher at the kiosk or cage for large denomination bills, or requests a casino check for what appears to be a legitimate winning credit from a slot machine.

— A customer frequently purchases chips with currency under a reportable threshold, engages in minimal play, and walks away without cashing out the chips.

— A customer transfers funds to a casino for deposit into a front money account, withdraws it in chips at the table and engages in minimal play, then requests the chips to be exchanged for a casino check.

- Unusual gaming and transaction patterns, such as:

— Two customers frequently bet large amounts to cover between them both sides of an even bet, such as:

> Betting both "red and black" or "odd and even" on roulette;

> Betting both "with and against" the bank in baccarat;

> Betting the "pass line" or "come line" and the "don't pass line" and "don't come line" in craps.

— A customer routinely bets both sides of the same line for sporting events (i.e., betting both teams to win), and thus the amount of overall loss to the customer is minimal (known as "hedging").

— A customer requests the issuance of a casino check payable to third parties, or without a specified payee.

— A customer makes large deposits or pays off large markers with multiple instruments (cashier's checks, money orders, traveler's checks or foreign drafts) in amounts of less than $3,000 indicating an attempt to avoid identification requirements.

— A customer withdraws a large amount of funds from a deposit account and requests multiple casino checks to be issued, each less than $10,000.

— A customer establishes a high value deposit that remains dormant for an extended period of time, then withdraws or transfers the funds.

The risk of money laundering comes not only from the specific behaviors, but also the type of customer casinos choose to conduct business with. Players often build a reputation of a high roller t as long as they show big play, without being subject to the due diligence necessary to determine the source of funds. The biggest mistake a casino can make is to allow play and accept the revenue without reasonably determining the source of gaming funds. US casinos may soon have to vet where their high rollers' funds come from under a requirement being developed by the US Treasury Department. While the existing rules do not explicitly require the source of funds to be known, it is recommended that casinos require more information from certain customers to shed light on high-risk transactions, such as international wire transfers and large cash deposits, as part of the risk-based approach.

The United States, through FinCEN, has been one of the most aggressive authorities on issuing anti-money laundering program deficiency penalties to some of the largest casinos in the industry:

- **Tinian Dynasty Hotel & Casino fined $75M (2015)** — Casino failed to develop and implement an AML program (no dedicated AML officer, failure to develop and implement AML policies and procedures, no independent tests of the AML program), which led the casino to fail to file thousands of CTRs and have employees assist wealthy VIP patrons engage in suspicious transactions (especially structuring).
- **Trump Taj Mahal fined $10M (2015)** — Casino failed to maintain an effective AML program, failed to file SARs and CTRs, and maintain appropriate records.
- **Caesar's Palace fined $9.5M (2015)** — Casino "allowed some of the most lucrative and riskiest financial transactions to go unreported," promoted private salons in the United States and abroad without appropriately monitoring transactions, such as wire transfers, for suspicious activity and openly allowed patrons to gamble anonymously.
- **Sparks Nugget fined $1M (2016)** — Casino "had a systemic breakdown in its compliance program" and disregarded its compliance manager. Rather than file rightfully prepared suspicious activity reports (SARs), Sparks Nugget instructed the compliance manager to avoid interacting with regulatory auditors and prevented her from reviewing a copy of the completed regulatory exam report.

In addition to ensuring adequate record-keeping and reporting requirements, casino AML/CFT programs should establish a process that will enable the casino to reasonably determine sources of funds and allow customer due diligence to be conducted at the time the funds are accepted, often with a customer already on property and ready to game, rather than relying exclusively on the after-the-fact back of house compliance investigation.

While the notion of on-demand enhanced know your customer (KYC) and source of fund questioning is relatively new to casinos, there are many ready-to-use tools developed specifically for the industry's front-of-house operations. The best processes will combine information from various international sources — criminal and judicial, securities and exchanges, financial, government and worldwide lists, political exposure, negative news, business associations — and ID verification, making the due diligence possible directly from the frontline of operations.

Case Study

In 2013, The US Department of Justice concluded its money laundering investigation into Las Vegas Sands Corp., resulting in a $47M settlement to avoid criminal prosecution in connection with funds gambled by high rollers in Las Vegas, particularly by Zhenli Ye Gon, a Chinese-Mexican businessmen who owned a pharmaceutical factory in Mexico.

Between 2006 and 2007, Ye Gon deposited over $50M at the Sands, principally via wire transfers and cashier's checks, which was allegedly proceeds of crime tied to the illegal manufacture of synthetic drugs; and received as much as $100M. In 2007, $207M cash was seized from Ye Gon's residence in Mexico, the largest-ever seizure of cash.

According to the evidence gathered by the DOJ, Ye Gon took steps to actively avoid detection of money laundering and used classic money laundering methods. Ye Gon and his associates wired money to the Sands and its subsidiary companies from two different banks and seven different Mexican money exchange houses known as casa de cambios. The wire originators included several companies and individuals the Sands could not link to Ye Gon to. According to the DOJ, Ye Gon also transferred funds from Mexican casas de cambios to Sands' subsidiary in Hong Kong for subsequent transfers to Las Vegas. In many instances, Ye Gon's wire transfers lacked sufficient information to identify him as the intended beneficiary. Additionally, Sands allowed Ye Gon to conduct several transfers of funds to an account that did not identify its association with the casino, specifically an aviation services account of Interface Employee Leasing, used to pay pilots operating the company's aircraft.

Casinos are not limited to physical locations. In fact, online casinos and gaming operations have increased their presence in recent years. Online gaming may be regulated in certain jurisdictions; however, a lot of online gaming companies operate illegally. For example, in the United Kingdom, the Gambling Commission requires a license for remote gambling where the business operates in the UK and any part of its gambling equipment is located in the UK or, if the equipment is located outside the UK, but the business operates through a British-facing business. Online gaming is also regulated in Antigua and Barbuda under the Interactive Gaming and Interactive Wagering Regulations and required to establish compliance programs.

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

Due to the inconsistent regulatory environment and susceptibility to cyber criminals, some credit card issuers no longer allow the use of its credit cards for online gambling. Financial institutions screen merchant codes that identify the type of business accepting the credit card and transaction codes for card not present (i.e., the cardholder is not physically in the casino to process the transaction via a card reader). The bank can thus block internet gambling transactions. However, online gambling can be funded in numerous ways beyond credit cards, such as prepaid cards, wire transfers, peer-to-peer transfer, virtual currency, and mobile phone carrier billing.

MONEYVAL is the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism. In its April 2013 research report entitled, "The Use Of Online Gambling For Money Laundering And The Financing Of Terrorism Purposes," identified numerous potential typologies for money laundering. Some examples include:

- A money launderer colludes with an operator of an offshore online gambling operation and deposits funds obtained from criminal activities into the gambling account and withdraws such funds as winnings. The website operator keeps a percentage of the proceeds as a commission while the launderer declares the winnings to the tax authorities and then uses the funds for legitimate purposes.

- A money launderer colludes with professional gamblers to place illegally obtained funds on online gambling websites. The gamblers keep a commission from any winnings made before transferring the remaining funds to the launderer.
- A money launderer deposits funds into an online gambling account by using a stolen identity. He or she bets using the funds and receives payouts for the winnings or sustains acceptable losses.

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

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

In July 2015, FATF released a report titled, "Money Laundering / Terrorist Financing Risks and Vulnerabilities Associated With Gold," which reinforced prior typology reports. Gold has high intrinsic value in a relatively compact and easy to transport form. It can be bought and sold easily and often with anonymity for currency in most areas of the world. It is more readily accepted than precious stones, especially since it can be melted down into many different forms. It holds its value regardless of the form it takes — whether as bullion or as a finished piece of jewelry — and is thus often sought after as a way of facilitating the transfer of wealth. For some societies, gold carries an important cultural or religious significance that adds to its demand.

Here are two of the key findings from the report:

1) Gold is an extremely attractive vehicle for laundering money. It provides a way for criminals to convert their illicit cash into anonymous, transferable assets.
2) The gold market is a target for criminal activity because it is lucrative. Understanding and knowing the various stages of the gold market and types of predicate offenses is critical in identifying money laundering.

   Case Study

   In 'Operation Meltdown,' US Homeland Security Investigations (HSI) investigators uncovered a carousel scheme in which jewelers were converting the proceeds from drug sales into the equivalent value in gold. The scheme involved a criminal organization with links to gold suppliers in the New York area that were laundering millions of dollars in drug proceeds. The HSI investigation disclosed that the exported gold from Colombia was described as "gold pigments" and upon importation into the United States the same merchandise was then described as "gold bullion." The gold bullion was then transported to New York, where jewelers who were cooperating with drug trafficking organizations disguised the gold in a wide range of common objects like wrenches, nuts, bolts, belt buckles and trailer hitches. These items were exported back to Colombia at a declared value far below the worth of their weight in gold. Upon arrival in Colombia, the same gold was recast into bullion and exported again to the US as "gold pigment."

The investigation of this case resulted in the arrest of 23 jewelers charged with money laundering and others, along with the seizure of 140 kg of gold, more than 100 loose diamonds, USD$2.8 million, 118 kg of cocaine, 6 guns and 2 vehicles.

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

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

- **Payments or returns to persons other than the owner:** If one person delivers precious metal for refining and asserts ownership of the metal and authority to sell it, but directs payments to be made to another person, that transaction may be questionable. The "dealer in precious metal" is being used to transfer an asset not only from one form into another — unrefined gold to refined gold or money within the international finance system — but also from one person to another.
- **Precious metal pool accounts:** These accounts are maintained by a small number of large and sophisticated precious metal companies and have worldwide scope. They receive and hold precious metal credits for a customer, which can be drawn on by that customer. The customer can request the return of the precious metals, the sale and return of monetary proceeds, or the delivery of precious metal to another person. Thus, a refining customer in one country can deliver gold scrap for refining, establish a gold credit in the refiner's pool account system, and subsequently have delivery made by the refiner to another person, based upon that credit.

  Case Study

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

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

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

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

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

Case Study

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

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

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

TRAVEL AGENCIES

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

Case Study

Operation Chimborazo, named for the famous Ecuadorean mountain, was a large multinational effort in the mid-1990s aimed at businesses suspected of laundering drug proceeds. The operation focused on the money laundering organization of Hugo Cuevas Gamboa, a reputed principal launderer for the Cali Cartel. In 1994, law enforcement teams cracked down on several businesses in Latin American countries, which included travel agencies. During a raid in Argentina, the authorities arrested the owners of a travel agency that was part of an organization that laundered $50 million per week in drug proceeds from 22 countries.

Money laundering can occur in travel agencies in the following manner:

- Purchasing an expensive airline ticket for another person who then asks for a refund.
- Structuring wire transfers in small amounts to avoid record-keeping requirements, especially when the wires are from foreign countries.
- Establish tour operator networks with false bookings and documentation to justify significant payments from foreign travel groups.

VEHICLE SELLERS

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

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

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

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

There have also been cases where authorities have charged that a car dealer laundered money by allowing a drug dealer to trade in his cars for cheaper models and to be paid in checks, not cash, for the difference. In one such “down-trading” money laundering scheme, a drug dealer traded in his $37,000 Porsche for a $17,000 Ford Bronco and the car dealer allowed the down-trade, knowing that the customer was a drug dealer, in violation of the anti-money laundering law.

Case Study

In 2011, The US Department of the Treasury identified the Lebanese Canadian Bank SAL together with its subsidiaries (LCB) as a financial institution of primary money laundering concern for the bank’s role in facilitating the money laundering activities of an international narcotics trafficking and money laundering network. The US authorities determined that LCB — through

management complicity, failure of internal controls, and lack of application of prudent banking standards — had been used extensively by persons associated with international drug trafficking and money laundering network.

In this network, a US designee Ayman Joumaa coordinated the transportation, distribution and sale of multi-ton bulk shipments of cocaine from South America, and laundered the proceeds — as much as $200 million per month — from the sale of cocaine in Europe and the Middle East. The proceeds were laundered through various methods, including through car dealerships. Specifically, Ayman Joumaa deposited bulk cash into multiple exchange houses, including the one that he owned, which then deposited the currency into their LCB accounts. He or the exchange houses then instructed LCB to perform wire transfers to move some of the funds through LCB's US correspondent accounts via suspiciously structured electronic wire transfers to multiple US-based used car dealerships — some of which were operated by individuals who have been separately identified in drug-related investigations. The recipients used the funds to purchase vehicles in the United States, which were then shipped to West Africa and/or other overseas destinations, with the proceeds ultimately repatriated back to Lebanon.

GATEKEEPERS: NOTARIES, ACCOUNTANTS, AUDITORS, AND LAWYERS

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

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

In the European Union and several other countries, mandatory anti-money laundering duties already apply to gatekeepers. FATF's 40 Recommendations also cover independent legal professionals *(see Chapter 3 for more on the Recommendations)*, including lawyers and legal professionals and other gatekeepers.

In its 2013 typology report, FATF stated that the following functions provided by lawyers, notaries, accountants and other professionals are the most useful to a potential money launderer:

- Creating and managing corporate vehicles or other complex legal arrangements, such as trusts. Such arrangements may serve to obscure the links between the proceeds of a crime and the perpetrator.
- Buying or selling property. Property transfers serve as either the cover for transfers of illegal funds (layering stage) or the final investment of proceeds after they pass through the initial laundering process (integration stage).
- Performing financial transactions. Sometimes these professionals may carry out various financial operations on behalf of the client (for example, issuing and cashing checks, making deposits, withdrawing funds from accounts, engaging in retail foreign exchange operations, buying and selling stock, and sending and receiving international funds transfers).

- Providing financial and tax advice. Criminals with large amounts of money to invest may pose as individuals hoping to minimize tax liabilities or seeking to place assets out of reach in order to avoid future liabilities.
- Providing introductions to financial institutions.
- Undertaking certain litigation.
- Setting up and managing a charity.

In many cases, criminals will use legal professionals to provide an impression of respectability in order to dissuade questioning or suspicion from financial institutions, and to create an added step in the chain of any possible investigations. Additionally, legal professionals may deliberately misuse a client's legitimate accounts to conduct transactions without the client's knowledge.

The report also describes red flag indicators of money laundering of terrorism financing:

1. The client:
    a. Is overly secretive.
    b. Is using an agent or an intermediary or avoids personal contact without a good reason.
    c. Is reluctant to provide or refuses to provide information or documents usually required to enable the transaction's execution.
    d. Holds or has previously held a senior public position, or has professional or family ties to such individuals.
    e. Is known to have been the subject of investigation for an acquisitive crime (i.e., one where the offender derives material gain from the crime, such as theft or embezzlement).
    f. Is known to have ties to criminals.
    g. Shows unusual interest and asks repeated questions on the procedures for applying ordinary standards.
2. The parties:
    a. Are native to, or residents in, or are incorporated in a high-risk country.
    b. Are connected without an apparent business reason.
    c. Are tied in a way that generates doubts as to the real nature of the transaction.
    d. Appear in multiple transactions over a short period of time.
    e. A re incapacitated or under legal age and there is no logical explanation of their involvement.
    f. Attempt to disguise the real owner or parties to the transaction.
    g. Are not directing the transaction. Rather, the person directing the operation is not one of the formal parties to the transaction.
    h. Does not appear to be a suitable representative.

3. The source of funds:
    a. Is provided using unusual payment arrangements.
    b. Is collateral located in a high-risk country.
    c. Represents a significant increase in capital for a recently incorporated company, including foreign capital, without a logical explanation.
    d. Represents unusually high capital in comparison with similar businesses.
    e. Stems from a security transferred with an excessively high or low price attached.
    f. Stems from large financial transactions that cannot be justified by the corporate purpose.
4. The lawyer:
    a. Is at a significant distance from the client or transaction without a legitimate or economic reason.
    b. Does not have experience in providing the particular services needed.
    c. Is being paid substantially higher than usual fees without a legitimate reason.
    d. Is frequently changed by the client, or the client has multiple legal advisors without legitimate reason.
    e. Is providing services previous refused by another professional.
5. The retainer involves:
    a. Transactions that are unusual with regards to the type of operation and the transaction's typical size, frequency or execution.
    b. Transactions that do not correspond to the client's normal business activities and shows that he does not have a suitable knowledge of the nature, object or the purpose of the professional performance requested.
    c. The creation of complicated ownership structures or structures with involvement of multiple countries when there is no legitimate or economic reason.
    d. A client transaction history that does not have documentation to support company activities.
    e. Inconsistencies and unexplained last minute changes to instructions.
    f. No sensible commercial/financial/tax reason for the transactions or increased complexity that unnecessarily results in higher taxes or fees.
    g. Exclusively keeping documents or other goods, holding large deposits, or otherwise using the client account without provision of legal services.
    h. Abandoned transactions without concern for fee level or after the receipt of funds.
    i. A power of attorney sought for the administration or disposal of assets under unusual circumstances without logical reason.

j. Litigation that is settled too easily or quickly with little or no involvement of legal professional retained.

k. Requests for payments to third parties without substantiating reason or corresponding transaction.

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

Case Study

An Eastern European was acting under an alias as the director of a company for which he opened an account with a Belgian bank. Transfers were made to this account from abroad, including some on the instructions of "one of our clients." The funds were then used to issue a check to a notary for the purchase of a property. The notary was drawn to the fact that some time after the purchase, the company went into voluntary liquidation, and the person concerned bought the property back from his company for an amount considerably above the original price. In this way the individual was able to insert money into the financial system for an amount corresponding to the initial sale price plus the capital gain. He was thus able to use a business account, front company customer, purchase of real estate, cross-border transaction and wire transfers to launder money that, according to police sources, came from activities related to organized crime. It appeared that the company acted as a front set up merely for the purpose of carrying out the property transaction.

Case Study

An attorney was convicted by a jury of conspiracy to commit money laundering. The attorney helped to invest the drug proceeds of his client by forming a corporation in the name of the client's wife and arranging a loan from the corporation to another (non-criminal) client. He then drafted a phony construction work contract, making the repayment of the loan appear to be payment for construction work performed by the company. He also drew up a promissory note, which the wife signed, but did not provide copies of the note to either party. The attorney also advised his client how to deposit the cash from the loan without triggering reporting requirements. The appeals court upheld the attorney's conviction but remanded him for resentencing after finding that the district court abused its discretion by not applying a sentencing enhancement based on the attorney's use of "special skills" (legal skills) in committing the offenses of conviction.

The issue of requiring attorneys to be gatekeepers in the AML/CFT area has been controversial due to the fact that attorneys have confidential relationships with their clients. Various alternatives have been discussed and debated, including:

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

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

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

INVESTMENT AND COMMODITY ADVISORS

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

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

Transactions of multiple account holders are combined and their identities are unknown to the holding FCM.

Commodity trading advisors ("CTA") engage in the business of advising others, either directly or indirectly, as to the value or advisability of trading futures contracts, commodity options and/or swaps, issue analyses or reports concerning trading futures or commodity options. CTAs are also responsible for trading of managed futures accounts. By directing such accounts, CTAs 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 should implement compliance programs to detect and deter such activity.

Other positions 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.
- 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-C: 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.
  - — Independent introducing broker: A broker that is subject to minimum capital and financial reporting requirements. This type of broker may introduce accounts to any FCM.
- Investment adviser: Provides advice on securities and investments and manages client assets.

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

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

TRUST AND COMPANY SERVICE PROVIDERS

Trust and company service providers (TCSPs) participate in the creation, administration or management of corporate vehicles. They refer to any person or business that provides any of the following services to third parties:

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

In a 2010 report called, "Money Laundering Using Trust and Company Service Providers," FATF found that, in many jurisdictions the existence of TCSPs is not recognized. However, in these jurisdictions, trust and company services may well be provided by lawyers and other professionals who are already regulated. For example, in many jurisdictions, lawyers will be engaged in the formation of companies for clients to hold assets (e.g., a yacht, a residential or commercial property) outside of that client's jurisdiction. FATF noted that some TCSPs are required to afford confidentiality privileges to a client, which can conflict with AML reporting requirements.

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

The 2010 FATF report, "Money Laundering Using Trust and Company Service Providers" provides the following vulnerabilities and red flags for this industry:

- Unknown or inconsistent application of regulatory guidelines regarding identification and reporting requirements.
- Limited market restriction on practitioners to ensure adequate skills, competence and integrity.
- Inconsistent record-keeping across the industry.
- TCSPs may operate in an unlicensed environment.
- Depending on the jurisdictional requirements, a TCSP's CDD may be performed by other financial institutions.

Some potential indicators of money laundering for this industry include the following:

- Transactions that require the use of complex and opaque legal entities and arrangements.
- The payment of "consultancy fees" to shell companies established in foreign jurisdictions or jurisdictions known to have a market in the formation of numerous shell companies.
- The use of TCSPs in jurisdictions that do not require TCSPs to capture, retain, or submit to competent authorities information on the beneficial ownership of corporate structures formed by them.
- The use of legal persons and legal arrangements established in jurisdictions with weak or absent AML/CFT laws and/or poor record of supervision and monitoring of TCSPs.
- The use of legal persons or legal arrangements that operate in jurisdictions with secrecy laws.
- Multiple intercompany loan transactions or multi-jurisdictional wire transfers that have no apparent or legal purpose.

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

Regulations should stipulate how the service provider conducts its business, including how directors selected by the provider meet their obligations as trustees or trusteeships. In its 2004 report, Transparency International stated that the first jurisdiction to bring these activities under regulatory control was Gibraltar, which enacted legislation in 1989. Some other offshore jurisdictions have either introduced some form of regulatory control or will in the future.

Regulations are not uniform; they range from a simple minimum capitalization requirement to full regulatory oversight. Often, the scope of the legislation is limited, excluding certain types of activities. Sometimes, the legislation bars regulators from gaining access to client files without client permission (or a court order), thereby making checks on the adequacy of the license-holder's CDD provisions virtually impossible. Furthermore, while some jurisdictions include service providers within their AML regulations — for example, by making compliance with the regulations a condition of licensing — many do not, leaving service providers free of any AML duties beyond those imposed

upon the general public. As a result of these differing standards, it is easy for a person seeking to use a company or trust for criminal purposes to select a jurisdiction that either lacks requirements or has only inadequate ones, said Transparency International.

REAL ESTATE

The real estate sector is frequently used in money laundering activities. Investing illicit capital in real estate is a classic method of laundering dirty money, particularly in countries with political, economic and monetary stability.

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. Countless real estate and business deals are closed every day using escrow funds. They are attractive to money launderers because of the large number of diverse transactions that can pass through them in any deal; escrow accounts can facilitate the movement of funds by cashier's checks, wire transfers or company checks to seemingly legitimate individuals or companies. Given the large amounts of activity that might be expected in an escrow account, a money launderer could easily disguise illegal activity in the account while appearing to operate the account in a manner consistent with what would be expected.

Many real estate transactions involve the deposit of a large check from the mortgagee, as well as checks and cash required from the buyer at closing (however, as discussed later in this section, cash purchases of real estate are becoming more prevalent). 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. Ultimately, monies may be paid outright by the escrow agent as cashier's checks obtained by him, as wire transfers, or as corporate or escrow checks to straw men or shell corporations. Each closing also entails numerous routine disbursements for the payment of the proceeds to the seller, payoff of the mortgage, real estate commissions, taxes, satisfaction of liens, and other payments. To a bank and other observers, the disbursement of funds at a closing may appear to be one legitimate set of transactions. Money laundering can be easily hidden because the size and volume of routine escrow account activity smooths out the "spikes" (i.e., the ups and downs in an account) or multiple deposits associated with money laundering.

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

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.

In April 2008, FinCEN published, "Suspected Money Laundering in the Real Estate Industry," an assessment based on suspicious activity report (SAR) filing analysis. The report makes a distinction between fraudsters and money launderers. Lenders are likely to file a SAR when they are the target of failed or successful mortgage fraud schemes that threaten the institution's revenues, but may have significant difficulty detecting mortgage loan fraud perpetrated by money launderers. This is because money launderers strive to project the image of normalcy by integrating illicit funds through regular and timely payments. For example, only about 20 percent of SAR filings associated with the residential real estate industry reportedly described suspected structuring and/or money laundering.

In a 2015 brief, the Australian Transaction Reports and Analysis Centre (AUSTRAC) identified real estate to be a significant money laundering channel in Australia. The brief cites confiscations involving money laundering totaling over AUD$23M between 2012 and 2013. According to the brief, real estate is an attractive channel for laundering illicit funds because:

- It can be purchased with cash.
- The ultimate beneficial ownership can be disguised.
- It is a relatively stable and reliable investment.
- Value may be increased through renovations and improvements.

Money laundering through real estate can be relatively uncomplicated compared to other methods and requires little planning or expertise. Large sums of criminal proceeds may be integrated into the legitimate economy through real estate investments (placement and layering phases). Properties may also be sold for a profit or retained for residential, investment or vacation purposes (integration phase).

In Australia, common money laundering methods involving real estate:

- Use of third party straw buyers described as "cleanskins."
- Use of loans and mortgages as a cover for laundering, which may involve lump sum cash repayments to integrate illicit funds into the economy.
- Manipulation of property values to disguise undisclosed cash payments through over- or under-valuing or "flipping" through successive sales to increase value.
- Structuring cash deposits used for the purchase.
- Generation of rental income to legitimize illicit funds.
- Conducting criminal activity, such as the production of cannabis or synthetic drugs, at the purchased property.
- Use of illicit cash to make property improvements to increase the value and profits at sale.
- Use of front companies, shell companies, trust and other company structures to hide beneficial ownership and obvious links to criminals.
- Use of gatekeepers such as real estate agents, conveyancers or solicitors to conceal criminal involvement, complicate the money laundering process and provide a veneer of legitimacy to the transaction.

- Investment by overseas-based criminals to conceal assets and avoid confiscation from authorities in their home jurisdiction.

The report cites methods for detecting money laundering through real estate where transactions intersect with the regulated AML/CFT sector, such as when real estate transactions involve financial institutions in the form of loans, deposits or withdrawals. It also outlines red flags that should prompt further monitoring and examination, particularly when multiple indicators are present. These red flags include:

- Various uses of cash to aggregate funds for property purchase or down payment or to repay loans.
- Multiple purchases and sales in a short period of time, sometimes involving property over- or under-valuation or straw buyers
- Use of off-shore lenders
- Unknown sources of funds for purchase such as incoming foreign wires where the originator and beneficiary customer are the same
- Ownership is the customer's only link to the country in which the real estate is being purchased.

In its five-part "Towers of Secrecy" series published in 2015, the New York Times pierced the secrecy of more than 200 shell companies that have owned condominiums at the Time Warner Center, a high-end property located in the heart of Manhattan. In the investigative series, the newspaper found that nearly half of the most expensive residential properties are now purchased through shell companies throughout the United States. At the Time Warner Center, 37 percent of the condos are owned by foreigners, at least 16 of which have been the subject of governmental inquiries, including housing and environmental fraud. The foreign owners have included government officials and close associates of officials from Russia, Colombia, Malaysia, China, Kazakhstan and Mexico and they mainly used limited liability companies for the purchases. Oftentimes, signatures on the property documents were illegible, blank, or signed by a lawyer with the lawyer's contact information registered.

The paper points out that there are no legal requirements for the real estate industry in the United States to identify beneficial owners or examine their backgrounds. In 2016 (subsequent to the *New York Times* series), FinCEN began issuing a series of Geographic Targeting Orders (GTOs) to help law enforcement identify individuals acquiring luxury residential properties through limited liability companies or other opaque structures without the use of bank financing. During the 180 days of each outstanding GTO, US title insurance companies are required to identify the natural persons behind shell companies used to pay all cash for high-end residential real estate in specified US metropolitan areas that exceed specified dollar amounts prescribed for each area. It is important to note that in this context "all cash" refers to transactions that do not involve traditional financing and does not necessarily reference the use of physical cash.

International Trade Activity

International trade activity is critical to an integrated economy and involves numerous components that can be manipulated for the benefit of money launderers and terrorist financiers such as banks, currency exchange, free trade zones, cross-border payments, ports, invoices, goods, shipments, shell companies and credit instruments that oftentimes are inherently complex transactions. Trade-based money laundering and the black market peso exchange are two significant money laundering techniques that have proven successful in illicit finance. Typically, free trade zones are manipulated in both techniques.

FREE TRADE ZONES

With more than 3,000 free trade zones (FTZs) in over 135 countries, FTZs play an integral role in international trade. FTZs are designated geographic areas with special regulatory and tax treatments for certain trade-related goods and services. FTZs are often located in developing countries near ports of entry but are separate from traditional ports of entry and typically operate under different rules. Most major FTZs are also located in regional financial centers that link international trade hubs with access to global financial markets. Examples of FTZs are the Colon Free Trade Zone in Panama and the Shanghai Free Trade Zone (officially the China Pilot Free Trade Zone) in China.

According to FATF's March 2010 Report on the Money Laundering Vulnerabilities in Free Trade Zones, systemic weaknesses for FTZs include:

1. Inadequate AML/CFT safeguards.
2. Minimal oversight by local authorities.
3. Weak procedures to inspect goods and legal entities, including appropriate record-keeping and information technology systems.
4. Lack of cooperation between FTZs and local customs authorities

The relaxed oversight in FTZs makes it more challenging to detect illicit activity and provides an opportune setting for trade-based money laundering schemes. Moreover, FATF noted that some FTZs are as large as cities, which makes it difficult to effectively monitor incoming and outgoing cargo as well as repackaging and relabeling. Some FTZs export billions of dollars annually but have few competent authorities available to monitor and examine cargo and trade transactions.

TRADE-BASED MONEY LAUNDERING TECHNIQUES

When men's briefs and women's underwear enter a country at prices of $739 per dozen, missile and rocket launchers export for only $52 each, and full toilets ship out for less than $2 each, one should notice the red flags. These manipulated trade prices represent money laundering, tax evasion and/or terrorist financing.

In a June 2006 report, called "Trade-Based Money Laundering," FATF defined trade-based money laundering (TBML) as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins. In practice, this can

be achieved through the misrepresentation of the price, quantity or quality of imports or exports. Moreover, trade-based money laundering techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail.

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

The 2006 FATF study concluded that TBML 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.

According to the Guidance Paper on Combating Trade-based Money Laundering, February 1, 2016, developed by the Hong Kong Association of Banks with input from the Hong Kong Monetary Authority, understanding the commercial purpose of any trade transaction is a key requirement in determining its money laundering risk. The Guidance refers to six ways to execute trade-based money laundering:

1. **Over-invoicing or Under-invoicing:**
    - Over-invoicing: By invoicing the goods or service at a price above the fair market price, the seller is able to receive value from the buyer (i.e., the payment for the goods or service will be higher than the value that the buyer receives when it is sold on the open market).
    - Under-invoicing: By invoicing the goods or service at a price below the fair market price, the seller is able to transfer value to the buyer (i.e., the payment for the goods or service is lower than the value that the buyer will receive when it is sold on the open market).
2. **Over-shipping or Short-shipping:** The difference in the invoiced quantity of goods and the quantity of goods that are shipped whereby the buyer or seller gains excess value based on the payment made.
3. **Ghost-shipping:** Fictitious trades where a buyer and seller collude to prepare all the documentation indicating goods were sold, shipped and payments were made, but no goods were actually shipped.
4. **Shell companies:** Used to reduce the transparency of ownership in the transaction.
5. **Multiple Invoicing:** Numerous invoices are issued for the same shipment of goods, thus allowing the money launderer the opportunity to make numerous payments and justify them with the invoices.
6. **Black market trades:** Commonly referred to as the Black Market Peso Exchange whereby a domestic transfer of funds is used to pay for goods by a foreign importer.

Letters of credit are another vehicle for money laundering. Letters of credit are a credit instrument issued by a bank that guarantees payments on behalf of its customer to a third party when certain conditions are met. Letters of credit are commonly used to finance export because exporters want assurance that the ultimate buyer of its goods will make payment, and this is given by the buyer's purchase of a bank letter of credit. The letter of credit is then forwarded to a correspondent bank in the jurisdiction in which the payment is to be made. The letter of credit is drawn on when the goods are loaded for shipping, received at the importation point, clear customs and are delivered. Letters of credit can be used to facilitate money laundering by transferring money from a country with lax exchange controls, thus assisting in creating the illusion that an import transaction is involved. Moreover, letters of credit can also serve as a façade when laundering money through the manipulation of import and export prices. Another method of using letters of credits illicitly is in conjunction with wire transfers to bolster the legitimate appearance of non- existent trade transactions.

In July 2012, the Asia/Pacific Group on Money Laundering (APG) issued the "APG Typology Report on Trade Based Money Laundering," which reaffirmed the conclusions of the 2006 FATF study. The APG study cited the lack of reliable statistics relating to TBML as a major obstacle in devising strategies to tackle it. To assist in recognizing the multiple forms of TBML, the paper enumerates specific characteristics and red flags associated with jurisdictions, goods, corporate structures and predicate offenses.

It concluded that any strategy to prevent and combat TBML needs to be based on dismantling TBML structures, while allowing genuine trade to occur unfettered. It calls for an integrated, holistic approach, with an emphasis on interagency coordination and international cooperation to standardize data and statistics, create domestic task forces, deliver TBML-focused training, and conduct further research.

Case Study

In February 2011, the US Department of the Treasury designated the Lebanese Canadian Bank (LCB) as a financial institution of primary money-laundering concern, asserting that Hezbollah derived financial support from drug and money laundering schemes, including TBML. The TBML component of the operations involving consumer goods worldwide, including used cars purchased in the United States and shipped to West Africa for re-sale, with a portion of the proceeds allegedly funneled to Hezbollah.

In May 2014, FinCEN issued an advisory on the use of funnel accounts and trade-based money laundering. The advisory was the result of the possible impact of the 2010 Mexican law that restricted cash deposits of US dollars in Mexican banks. Subsequently, the restrictions were expanded to include similar deposits made at exchange houses (casas de cambio) and brokerages (casas de bolsa) in Mexico. Furthermore, additional guidance was issued by FinCEN based on bulk cash smuggling trends based on the restrictions that indicated an increase in the use of funnels accounts to move illicit proceeds of Mexico-related criminal organizations.

FinCEN defines a funnel account as, "an individual or business account in one geographic area that receives multiple cash deposits, often in amounts below the cash reporting threshold, and from which the funds are withdrawn in a different geographic area with little time elapsing between the deposits and withdrawals." Ways to identify possible funnel account activity include:

- An account opened in one US state receives numerous cash deposits of less than $10,000 (the currency reporting requirement) by unidentified persons at branches outside of the geographic region where the account is domiciled.
- Business account deposits take place in a different geographic region from where the business operates.
- Individuals opening or making deposits to funnel accounts lack information about the stated activity of the account, the account owner, or the source of the cash.
- A business account receives out-of-state deposits with debits that do not appear to be related to its business purpose.
- Notable differences in handwriting on the payee and amount lines than the signature line on checks issued from an account that receives out-of-state cash deposits.
- Wire transfers or checks issued from a funnel account are deposited into, or cleared through, the US correspondent account of a Mexican bank.

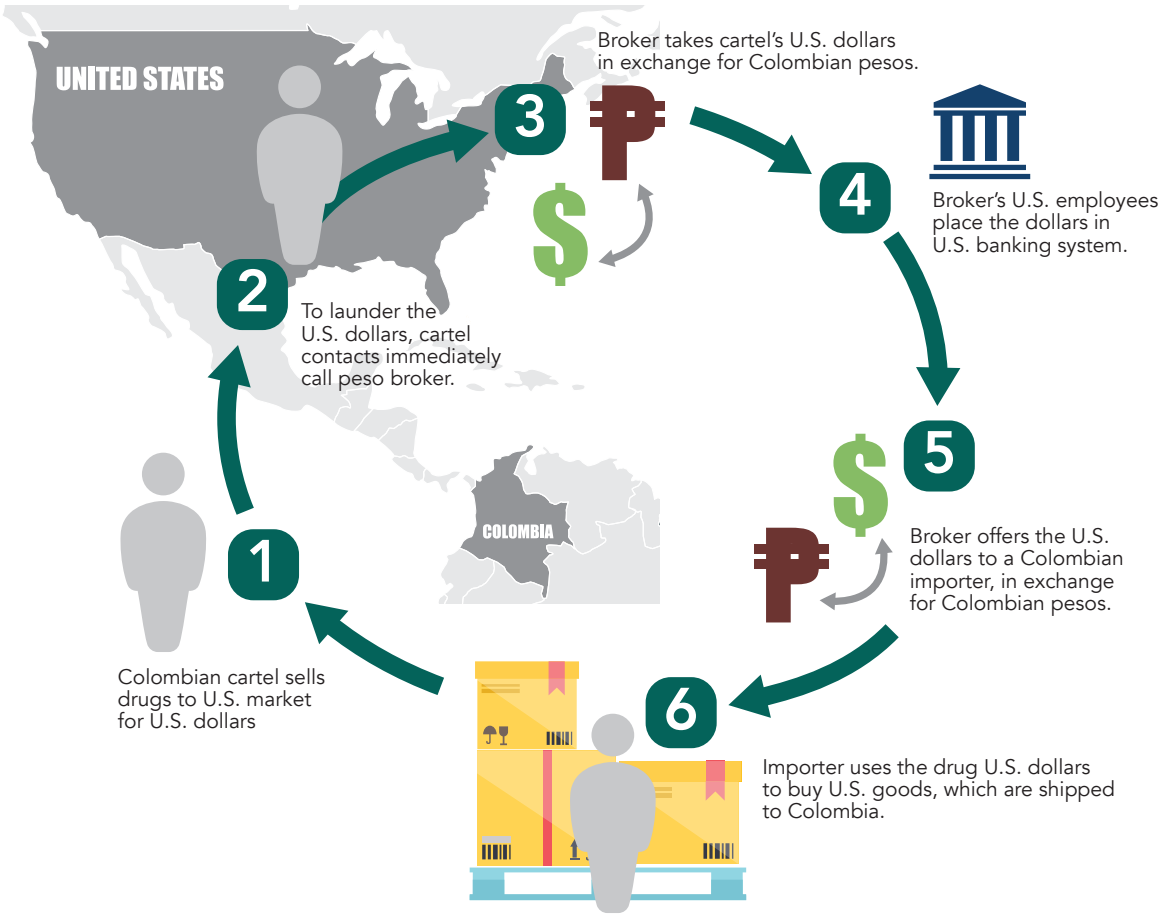
BLACK MARKET PESO EXCHANGE

A form of trade-based money laundering, the Black Market Peso Exchange (BMPE) is a process by which money in the United States derived from illegal activity is purchased by Colombian peso brokers and deposited in US 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 US. While the US is prominently figured in BMPE, the process is not limited exclusively to it.

Colombian importers created the BMPE in the 1950s as a mechanism for buying US dollars on the black market to avoid domestic taxes and duties on the official purchase of US dollars and on imported goods purchased with dollars. In the 1970s, Colombian drug cartels began using the BMPE to convert drug dollars earned in the US 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.

In FinCEN's February 18, 2010 Advisory to US Financial Institutions on Trade Based Money Laundering, it indicated that black market currency exchange systems have evolved beyond the Colombian BMPE method, mainly because of increased diligence by US banks. A common method used for initial placement of illicit funds into the financial system was structured deposits in the form of cash, money orders or other financial instruments. However, money launderers are currently utilizing individuals or businesses that have control over numerous bank accounts at numerous banks to bulk cash smuggle from the United States. The smuggled US dollars are deposited into foreign institutions — often in Mexico, but also in Central and South American countries — and wired back to the US and other prominent trade countries as payments for international trade goods and services.

Black Market Peso Exchange Example



According to the US Department of Justice in its April 24, 2014 press release on the prison terms for the owners of an import-export company that was used to move millions of dollars linked to illegal activity from the US to Mexico, the following is a typical BMPE scenario involving the US and Mexico:

> A peso broker works with an individual engaged in illegal activity, such as a drug trafficker, who has US currency in the US that he needs to bring to Mexico and convert to pesos. The peso broker finds business owners in Mexico who buy goods from vendors in the US, such as XYZ Inc., and need dollars to pay for those goods. The peso broker arranges for the illegally obtained dollars in the US to be delivered to the US-based vendors, such as XYZ Inc., where they are used to pay for the goods purchased by the Mexico based customers. Once the goods are shipped to Mexico and sold by the Mexico-based business owner for pesos, the pesos are turned over to the peso broker, who then pays the drug trafficker in Mexico.

Case Study

In September 2014, extensive law enforcement operations revealed evidence of pervasive money laundering activities involving BMPE schemes throughout the Los Angeles, California Fashion District. The area includes over 2,000 businesses covering about 100 city blocks in downtown Los Angeles. Garment industry businesses in the fashion district were used to launder money for drug trafficking organizations (DTOs). Bulk cash proceeds from drug sales were used to purchase textile-related goods, which were shipped to Mexico and other countries. The proceeds from the sales of the exported goods were forwarded to the DTOs in the form of local currency. During the September 10, 2014, enforcement action, US Homeland Security Investigation special agents seized over $90M in currency, the largest single-day bulk cash seizure in US history. The seized cash was found at various residences and businesses stored in various places such as file boxes, duffel bags, backpacks and even in the trunk of a Bentley. FinCEN issued a Geographic Targeting Order (GTO) on September 26, 2014, that lowered cash thresholds and triggered additional record-keeping requirements on specified textile-related businesses in the LA Fashion District in an effort to disrupt the activities of DTOs.

Case Study

In April 2015, FinCEN issued a GTO that similarly lowered cash reporting thresholds and implemented additional record-keeping requirements for certain financial transactions for about 700 Miami-based electronics exporters. According to FinCEN, the GTO was designed to disrupt complex BMPE-related schemes employed by DTOs, including the Sinaloa and Los Zetas DTOs based in Mexico. Law enforcement investigations revealed that many of these businesses are exploited by sophisticated TBML/BMPE schemes in which drug proceeds in the US are converted into goods that are shipped to South America and sold for local currency and ultimately transferred to drug cartels. The GTO was designed to enhance the transparency of the covered businesses' transactions.

Risk Associated with New Payment Products and Services

The internet, new payment platforms, and electronic money have changed the way people conduct business, transact with each other, and how consumers buy products and services. Whereas a small corner shop was limited to servicing local consumers, it can now have a broader, global reach with an online business as well. Digital payment platforms have altered how a consumer and the regulatory environment view a merchant or funds transmission. The cheaper cost of technology and our globally interdependent society, increasingly highly skilled engineering-based workforce, and entrepreneurial drive have all contributed to the evolution of new payment products and services pushing the boundaries of how and where money is used. Generally, the risk posed by these new payment systems is relative to the functionality of the service and their funding mechanisms.

Prepaid Cards, Mobile Payments And Internet-Based Payment Services

In October 2006, FATF published a report that examined the ways in which money can be laundered through the exploitation of new payment methods, such as 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. In addition, cross-border providers of new payment methods may pose more risk than providers operating just within a particular country. The report recommended continued vigilance to further assess the impact of evolving technologies on cross-border and domestic regulatory frameworks.

Prepaid cards have the same characteristics that make cash attractive to criminals: they are portable, valuable, exchangeable and anonymous. Typically, prepaid products require the consumer to pay in advance for future purchases of goods and services. Each payment is subtracted from the balance of the card or product until the total amount is spent. Prepaid cards can be categorized as either open loop or closed loop. Open-loop prepaid cards, many of which are network branded by American Express, Visa or MasterCard, can be purchased and loaded with money by one person and used like regular debit cards by the same person or another person to make purchases or ATM withdrawals anywhere in the world. Closed-loop prepaid products are of limited use for a specific purpose or service, such as with a certain merchant or retailer, whether online or at a physical location. Prepaid cards may be either non-reloadable, that is purchased for a fixed amount that cannot be reloaded as the funds are depleted, or the cards can be reloadable, which permits adding additional funds on the card to replace what was previously spent.

While there are many different types of prepaid cards that are used in a variety of ways, the cards typically operate in the same way as a debit card and ultimately rely on access to an account. There may be an account for each card that is issued or, alternatively, there may be a pooled account that holds the prepaid funds 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 with pre-paid cards:

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

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

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

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

According to the Joint Money Laundering Steering Group's Guidance on E-Money Guidance (2012), electronic money is "a prepaid means of payment that can be used to make payments to multiple persons, where the persons are distinct legal or natural entities." Electric money products can be card-based or online account-based. They can be issued by banks, building societies, and specialist electronic money institutions. Examples of e-money include prepaid cards that can be used to pay for goods at a range of retailers, or virtual purses that can be used to pay for goods or services online. All UK e-money institutions are regulated by the UK Financial Conduct Authority (FCA)and are governed under the Electronic Money Regulations (2011), which requires compliance with all AML/CFT and sanctions requirements.

The Guidance identifies several risk factors inherent in e-money for money laundering and terrorist financing, including:

- High, or no, transaction limits.
- Frequent cross border transactions.
- Certain merchant activity with higher risk businesses such as gambling.
- Funding with unverified persons.
- Funding with cash that leaves no electronic trail to the source of funds.
- Funding with other electronic money that lacks verified persons and/or source of funds.
- Non-face to face transactional activity.
- Features that increase the functionality of the card in terms of how to execute transactions such as person to person, business to person, business to business, person to business.
- Ability of customer to hold numerous purses.
- Segmentation of the business value chain.

After the 2006 Typology Report, FATF issued a similar report in 2010. And as the market continued to evolve, FATF issued "Guidance For A Risk-Based Approach Prepaid Cards, Mobile Payments And Internet-Based Payment Services," in 2013. In the guidance, it identified numerous inherent risks with what it called new payment methods (NPMs) such as:

- **Non face-to-face relationships and anonymity:**
  - — NPMs can be used to quickly move funds around the world, to make purchases and access to cash through the ATM network.
  - — For prepaid cards anonymity can occur when the card is purchased, registered, loaded, reloaded or used.
  - — Prepaid cards can easily be passed on to third parties that are unknown to the issuer.
  - — Customers may be established through agents, online or through a mobile payment system.
  - — Increase the risk of identity fraud or customers providing inaccurate information potentially to disguise illegal activity in non face-to-face verification.
- **Geographical reach:**
  - — Open-loop prepaid cards usually permit payments at domestic and foreign points of sales through global payment networks.
  - — Prepaid card providers may be based in one country and sell their product internationally through agents or online.
  - — The compact size of prepaid cards makes them more vulnerable to misuse than cash in cross-border transportations.
  - — Mobile and online payment services can transfer funds globally.
  - — Different regulatory AML/CFT regimes may exist where payments originate versus where they are ultimately received.
- **Methods of funding:**
  - — Prepaid card risk is increased by allowing cash funding and the possibility of reloading without any limit on the value placed on the card.
  - — Use of prepaid cards as an alternative to the physical cross-border transportation of cash.
  - — Mobile and online payment services can be funded using numerous methods such as banks accounts, non bank methods such as money transmitters, electronic monies, virtual currencies.
- **Access to cash:**
  - — Use of ATM networks for prepaid cards that allow funding in one country and cash withdrawals in another.
  - — Increasing connectivity between mobile and online payment methods with prepaid cards to fund or withdraw in cash.
- **Segmentation of services:**
  - — Prepaid cards usually require several parties to execute transactions including the program manager, issuer, acquirer, payment network, distributor and agents.

- — Mobile and online services require coordination with numerous interrelated service providers who must partner with international counterparts to provide cross-border transactions.
- — Use of agents and relying on unaffiliated third parties for customer acquisition.
- — NPM providers maintain bank accounts and use the banking system for periodic transactions to settle accounts with agents or partners and the banks may not have visibility into the ultimate customer for the transaction.

The guidance also stated that the risk of money laundering and terrorist financing in NPMs may be mitigated when the following are considered:

- **Customer due diligence (CDD):**
  - — The need and to what extent CDD should be performed varies depending on the level of risk posed by the product.
  - — The greater the functionality of the NPM, the greater the need may be for more enhanced CDD.
  - — Corroborating customer information in non face-to-face verification using third party databases, but also using open-source information readily available on the internet or social media.
- **Loading, value and geographical limits:**
  - — Setting initial load limits.
  - — Setting geographical or reloading limitations.
  - — Limiting the functionality of a product to certain geographical areas.
  - — Limiting the functionality of a product for the purchase of certain goods and services.
  - — Consider establishing individual tiers of service provided to customers.
  - — For prepaid cards:
    - > Limits on loading, duration, and ability to make cash withdrawals.
    - > Limitations on the amount that is prepaid and accessible.
  - — For Mobile:
    - > Maximum amount allowed per single transaction.
    - > Maximum cash withdrawals.
    - > Frequency or cumulative value of transactions.
    - > Limits based on day/week /month/ year or a combination thereof.
- **Source of funding:**
  - — Consider limited allowable sources of funding for a specific product.
  - — Consider identification for cash-based funding depending on load or account limits.

- **Record-keeping, transaction monitoring and reporting:**
  - — Retain transaction records of payments and funds transfers.
  - — Retain identifying information on the parties to the transaction.
  - — Retain and identify any account(s) involved.
  - — Retain the date of the transaction and the amount involved.
  - — For Mobile, obtain the phone number of the sender and receiver.
  - — Implement and utilize transaction monitoring relevant typologies.

Virtual Currency

A virtual or digital currency (VC) is a medium of exchange that operates in the digital space. It can be converted into either a fiat (e.g., a government-issued currency) or it can be a substitute for real currency. There are two types of virtual currencies: centralized and decentralized. Centralized virtual currencies (e.g., formerly the Liberty Reserve) have a centralized repository and a single administrator. Decentralized (e.g., Bitcoin) VCs have no repositories or administrators but work as peer-to-peer media of exchange without any need for an intermediary. According to FATF's 2014 report, Virtual Currencies, Key Definitions and Potential AML/CFT Risks, VCs can also be distinguished between convertible VCs (i.e., Bitcoin and WebMoney) that have an equivalent value and can be exchanged in real currency, and non-convertible VCs (i.e., Q Coins and World of Warcraft Gold) that are intended to be specific to a particular domain.

Virtual currencies allow value to be able to be transmitted anywhere in the world without the requirement of a centralized bank or institutional authority. In 2009, the Bitcoin ecosystem was developed as a cryptographic protocol to transfer value through the peer-to-peer network without reliance on a centralized banking structure. Bitcoins are units of value transfer that are established as a virtual currency. Much like any financial instrument, a Bitcoin derives its value from what another party is willing to trade for that item. In the case of Bitcoins, there is a value that is expressed in fiat currency that is based upon economic and market forces. A Bitcoin can be expressed as an equivalent value in each locale's specific currency.

With the VC market gaining traction and an increase in individuals and businesses operating in the ecosystem, on March 18, 2013, FinCEN issued interpretative guidance on VCs that categorized the participants within the ecosystem into three segments:

- A User is a person that obtains virtual currency to purchase goods or services
- An Exchanger is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency
- An Administrator is a person engaged as a business in issuing a virtual currency, and who has the authority to redeem such virtual currency

The guidance states that Administrators or Exchangers of virtual currency are MSBs engaging in money transmission and must comply with the registration, reporting, record-keeping and other regulations applicable to money transmitters, such as maintaining a compliant AML program.

In a typical transaction scenario, a User has an established virtual wallet or an account with an Exchanger to conduct a transaction. The User acquires virtual currency from the Exchanger, which allows the User to transfer funds in and out of that account. In relation to Bitcoin, in a transfer between two individuals, no personally identifiable information is disclosed to the two individuals or to any third-party intermediaries. While each transaction is registered in the blockchain and the publicly available distributed ledger, which provides valuable information beyond a traditional cash-to-cash exchange, it does not provide the actual identities behind the corresponding wallets. Thus, know your customer (KYC) is an important component of a legitimate exchanger's AML program.

For those tracking the movement of illicit funds, ownership information may be unavailable, with only the wallet address of the previous sender provided. However, the underlying technology and public recording of transactions allows for wallet address association that assists investigators in piecing together the ownership puzzle. VC businesses that facilitate the use, purchase, and transfer of VCs are an important source for details related to wallet ownership and source of fund information.

The regulation of VC businesses varies globally, ranging from AML/CFT obligations for exchanges to the mere issuance of advisories to the financial sector on the risks posed by those businesses as customers. In some countries, the financial sector is prohibited from interacting with VC businesses entirely.

Case Study

Liberty Reserve was a web site out of Costa Rica that used digital currency (its own called "LR") for payment processing and money transmission. In May 2013, FinCEN issued a Notice of Finding under Section 311 of the USA PATRIOT Act that Liberty Reserve S.A. was a financial institution of primary money laundering concern. Later that month, the US shut down the website. At the time, Liberty Reserve had more than 5.5 million user accounts worldwide and had processed more than 78 million financial transactions with a combined value of more than $8B.

Liberty Reserve maintained more than 200,000 customers in the United States, yet never registered with FinCEN as an MSB. Liberty Reserve did not conduct verification of account registration for individuals using the system, asking only for a working e-mail address, and allowed an individual to open an unlimited number of accounts. By paying an additional "privacy fee," users could hide their internal unique account number when sending funds within the Liberty Reserve system. Once an account was established, Liberty Reserve virtual currency could be sent instantly and anonymously to any other account holder within the global system. Essentially, unverified account holders could use the site to transfer LR between other unverified accounts holders.

Accounts were funded using exchangers, third-party entities that maintained bulk quantities of LR that were purchased using traditional funding methods. The exchangers operated as unlicensed money transmitters. Technically, the design was to layer funds from the point of origin (traditional funding such as cash or wire transfers) through the exchangers into a digital currency, and then the digital currency could be used to purchase illicit goods or withdrawn out of Liberty Reserve using a different exchanger. In May 2016, the founder, Arthur Budovsky, was sentenced to 20 years in prison for running the money laundering enterprise. Four co-defendants pleaded guilty and two of the remaining conspirators remain at large.

Case Study

In September 2013, the US Department of Justice unsealed a criminal complaint charging the alleged owner and operator of Silk Road, a dark market website created in 2011 to enable its users to buy and sell illegal drugs, weapons, stolen identity information and other unlawful

goods and services anonymously and beyond the reach of law enforcement, with narcotics trafficking, computer hacking, and money laundering conspiracies. Silk Road operated as a global black-market cyber bazaar that brokered anonymous criminal transactions and was used by several thousand drug dealers and other unlawful vendors to distribute unlawful goods and services to over a hundred thousand buyers. In May 2015, Ross Ulbricht was sentenced in Manhattan federal court to life in prison in connection with his operation and ownership of the site. Bitcoin was the sole accepted currency on the Silk Road.

Corporate Vehicles Used to Facilitate Illicit Finance

Various forms of corporate vehicles exist and are used to facilitate the movement of illicit finance. For example, corporate vehicles can be misused for money laundering, bribery and corruption activity, sheltering assets, and tax evasion, among other uses. Vehicles such as corporations, partnerships, and trusts are all excellent methods to maximize anonymity of ownership as well as its actual purpose.

Public Companies and Private Limited Companies

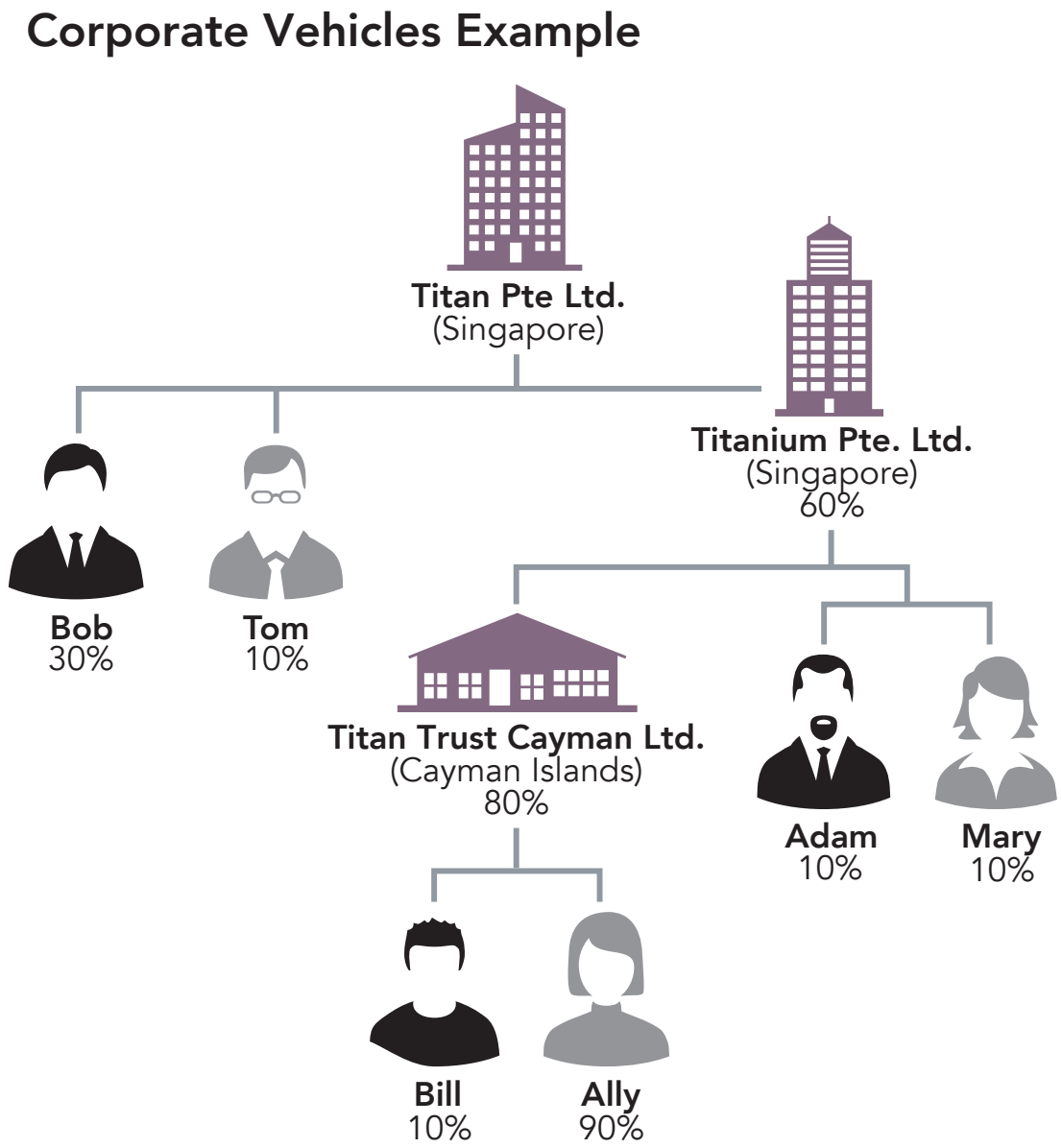
In most jurisdictions, corporate structure is distinguished between public companies and private limited companies. For public companies, shares are freely available and traded publicly, there is usually no limit to the number of shareholders, information on ownership and its board of directors is publicly available, and the companies are subject to significant regulation. On the other hand, private limited companies are not publicly traded, restrictive in the number of shares, ownership can be one or many, and are subject to minimal regulatory oversight.

A very common corporate vehicle subject to misuse is the limited liability company (LLC). The LLC is an attractive vehicle since LLCs can be owned or managed anonymously; virtually anyone can own or manage an LLC, including foreign persons and other business entities.

A member of an LLC is equivalent to a shareholder in a corporation. A manager, on the other hand, is equivalent to an executive officer or a member of the board of directors. An LLC may lack managers in which case the members manage the LLC. FinCEN has undertaken a number of activities to monitor LLCs better, as not every state (especially US domestic LLCs) is undertaking the same measures and controls towards LLCs (especially in the monitoring, recording and reporting of managers, ultimate beneficiaries and nominees).

International business corporations (IBCs) are entities formed outside of a person or businesses' country of residence, typically in offshore jurisdictions, for confidentially or asset protection purposes. IBCs permit the person to reduce transparency between its owner in his/her home country and that of the offshore entity where the company is registered. As a result, some benefits include asset protection, access to multiple investment markets, estate planning, legitimate tax benefits and serving as holding companies. The inherent risks with IBCs are that they are usually created in a tax haven and that they usually require incorporation with a local agent, who may further reduce the transparency of the IBC (e.g., serving as a nominee owner or director) and facilitate opening

accounts in the name of the IBC. Private investment companies (PICs) are established and used in a similar manner; however, they are typically limited to holding investment assets in tax-neutral offshore financial jurisdictions.



BEARER SHARES IN CORPORATE FORMATION

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

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

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

Bearer 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 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.

Shell and Shelf Companies

While shell companies may be created for legitimate purposes, they can also be established with the primary objective to claim the proceeds of crime as legitimate revenue and/or to commingle criminal proceeds with legitimate revenue. The use of shell and shelf companies to facilitate money laundering is a well-documented typology, according to FATF. FATF offers the following definitions:

- **Shelf company:** A corporation that has had no activity. It has been created and put on the shelf. This corporation is then later sold to someone who prefers a previously registered corporation over a new one.
- **Shell company/corporation:** A company that at the time of incorporation has no significant assets or operations.

In October 2006, FATF issued a report called, "The Misuse of Corporate Vehicles, Including Trust and Company Service Providers." In this report, FATF said that of particular concern was the ease with which corporate vehicles can be created and dissolved in some jurisdictions. It 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 by those involved in financial crime to conceal the sources of funds while keeping their ownership concealed.

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. Shell companies are often legally incorporated and registered by the criminal organization, but have no legitimate business. Often purchased "off the shelf" from lawyers, accountants or secretarial companies, they are convenient vehicles to launder money. 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. In addition, the information may be held by professionals who claim secrecy.

When FATF reviewed the rules and practices that impair the effectiveness of money laundering prevention and detection systems, it found in particular that shell corporations and nominees are widely used mechanisms to launder the proceeds from crime. A 2001 report, "Money Laundering in Canada: An Analysis of RCMP Cases," offered four related reasons to establish or control a shell company for money laundering purposes:

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

2. Through the use of shell companies, the launderer can create the perception that illicit funds have been generated from a legitimate source. Once a shell company is established, commercial accounts can be created at banks or other financial institutions. Especially attractive to money launderers are businesses that customarily handle a high volume of cash transactions, such as retail stores, restaurants, bars, video arcades, gas stations or food markets. 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.

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

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

Criminal enterprises also use real businesses to launder illicit money. These businesses differ from shell companies in that they operate legitimately, offering industrial, wholesale or retail goods or services. The Canadian report mentions the following money laundering techniques used in conjunction with criminally controlled companies:

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

- **Layering:** In some cases, a number of companies are established, many of them connected through a complex hierarchy of ownership. This helps to conceal criminal ownership and facilitates the transfer of illicit funds between companies, muddying any paper trail.
- **Loans:** Proceeds of crime can be laundered by lending money between criminally-controlled companies. In one case, a drug trafficker had $500,000 in a bank account in the name of a shell company. These funds were "lent" to restaurants in which the drug trafficker had invested. This seemingly legitimate use of the funds assisted in making it appear that the funds were being properly integrated into the economy. The $500,000 was repaid with interest to avoid suspicion.
- **Fictitious business expenses/False invoicing:** Once a criminal enterprise controls corporate entities in different jurisdictions, it can employ a laundering technique known as "double invoicing." An offshore corporation orders goods from its subsidiary in another country, and the payment is sent in full to the bank account of the subsidiary. Both companies are owned by the criminal enterprise and the "payment" for goods is actually a repatriation of illicit money previously spirited out of the country. Moreover, if the subsidiary has charged a high price for the goods, the books of the parent company will show a low level of profit, which means that the parent company will pay less in taxes. It can also work the other way around. An offshore corporation buys goods from a parent company at price that is too high. The difference between the real price and the inflated price is then deposited in the subsidiary's account.
- **Sale of the business:** When the criminal sells the business, he has a legitimate source of capital. The added benefit of selling a business through which illicit money circulates is that it will ostensibly exhibit significant cash flow and, as such, will be an attractive investment and will realize a high selling price.
- **Buying a company already owned by the criminal enterprise:** An effective laundering technique is to "purchase" a company already owned by the criminal enterprise. This laundering method is most frequently used to repatriate illicit money that was previously secreted to foreign tax havens. Criminal proceeds from offshore are used to buy a company that is already owned by the criminal enterprise. In this way, the launderer successfully returns a large sum of money that had been secreted out of the country.
- **Paying out fictitious salaries:** In addition to claiming the proceeds of crime as legitimate business revenue, criminally-controlled companies also help make certain participants in a criminal conspiracy appear to be legitimate by providing them with salaries.

Trusts

Trusts are private fiduciary arrangements that allow a grantor, or settlor, to place assets for future distribution to beneficiaries. The grantor/settlor will usually appoint a third party, a trustee, to administer the assets in accordance with the instructions provided in the trust document. Trusts are often seen as separate legal entities from the grantor; as such, they are often useful for estate planning and asset protection purposes. The instructions usually state how the grantor/settlor would like the funds to be distributed and are limited only to a legal purpose.

Trusts fall into one of two categories: revocable, in which case the grantor/settlor can terminate the trust; or irrevocable, in which case the grantor cannot terminate the trust once created. The flow of funds from the trust assets (the principal) to the beneficiaries can be in any of a number of ways, including providing them with the income generated by the principal, by providing fixed distributions of interest and/or principal or putting conditions on distributions (e.g., completing certain levels of schooling). Trusts will also name remaindermen who are designated to receive any residual assets after the conclusion of the trust's term (e.g., after the death of the grantor or the beneficiaries). Trusts allow a significant amount of flexibility and protection and have been used legitimately for centuries.

The significance of a trust account — whether onshore or offshore — in the context of money laundering cannot be understated. It can be used in the first stage of converting illicit cash into less suspicious assets; it can help disguise the 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.

In some jurisdictions trusts may be formed to take advantage of strict secrecy rules in order to conceal the identity of the true owner or beneficiary of the trust property. They are also used to hide assets from legitimate creditors, to protect property from seizure under judicial action, or to mask the various links in the money flows associated with money laundering or tax evasion schemes. For example, asset protection trusts (APTs) are a special form of irrevocable trust usually created (i.e., settled) offshore for the principal purposes of preserving and protecting part of one's wealth from creditors. Title to the asset is transferred to a person named the trustee. APTs are generally used for asset protection and are usually tax neutral. Their ultimate function is to provide for the beneficiaries. Some proponents advertise APTs as allowing foreign trustees to ignore US court orders and to simply transfer the trust to another jurisdiction in response to legal action threatening the trust's assets.

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

Lawyers often serve as trustees by holding money or assets "in trust" for clients. This enables lawyers to conduct transactions and to administer the affairs of a client. Sometimes, the illicit money is placed in a law firm's general trust account in a file set up in the name of the client, a nominee, or a company controlled by the client. Also, trust accounts are used as part of the normal course of a lawyer's duties in collecting and disbursing payments for real property on behalf of clients.

Terrorist Financing

After the terrorist attacks of September 11, 2001, the finance ministers of the Group of Seven (G-7) industrialized nations met on October 7, 2001, in Washington, D.C., and urged all nations to freeze the assets of known terrorists. Since then, many countries have committed themselves to helping disrupt terrorist assets by alerting financial institutions about persons and organizations that authorities determine are linked to terrorism. The G-7 nations marshaled FATF to hold an "extraordinary

plenary session" on October 29, 2001, in Washington to address terrorist financing. As a result, FATF issued the first eight of its Special Recommendations, which have since been incorporated into the current FATF Recommendations. *(See Chapter 2 for more detail.)*

Recommendation 5 encourages countries to criminalize terrorist financing and the financing of terrorist organizations and individual terrorists with or without a link to a specific terrorist act, as well as ensuring these crimes are designated as money laundering predicate offenses. This allows the application of money laundering statutes to terrorist financing and the potential for greater prosecution and deterrence. Cutting off financial support to terrorists and terrorist organizations is essential to disrupting their operations and preventing attacks.

DIFFERENCES AND SIMILARITIES BETWEEN TERRORIST FINANCING AND MONEY LAUNDERING

Money laundering and terrorist financing are often mentioned in the same breath, without much consideration to the critically important differences between the two. Many of the controls that businesses should implement are meant to serve the dual purposes of combating both money laundering and terrorist financing. The US 2015 Terrorist Financing Risk Assessment noted that controls instituted to combat money laundering have also strengthened our ability to identify, deter and disrupt terrorist financing. Of the individuals investigated by law enforcement for ties to terrorist organizations who had associated BSA records, 58 percent were reported as having engaged in suspected money laundering, including structuring.

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

The most basic difference between terrorist financing and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. The purpose of laundering funds intended for terrorists is to support terrorist activities. The individuals responsible for raising the funds are not the beneficiaries of the laundered funds. The money benefits terrorist activity. On the other hand, money laundering always involves the proceeds of illegal activity. The purpose of laundering is to enable the money to be used legally. The individuals responsible for the illegal activity are usually the ultimate beneficiaries of the laundered funds.

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; one reason being the continued and uncompromised future use of that source. In doing so, the terrorists use methods similar to those of criminal organizations: cash smuggling, structuring, purchase of monetary instruments, wire transfers, and use of debit, credit and/or prepaid cards. The hawala system,an informal value transfer system involving the international transfer of value outside the legitimate banking system and based on a trusted network of individuals, has also played a role in moving terrorist-related funds. In addition, money raised for terrorist groups is also used for mundane expenses like food and rent, and is not always strictly used for just the terrorist acts themselves.

DETECTING TERRORIST FINANCING

In its 2004 "Monograph on Terrorist Financing," the National Commission on Terrorist Attacks Upon the United States stated that neither the September 11 hijackers nor their financial facilitators were experts in the use of the international financial system. The terrorists created a paper trail linking them to each other and their facilitators. Still, they were adept enough to blend into the vast international financial system without revealing themselves as criminals. The money laundering controls in place at the time were largely focused on drug trafficking and large-scale financial fraud and were not sufficiently focused on the transactions engaged in by the hijackers. Since 9/11, international efforts to detect and deter terrorist financing have increased significantly. Conversely, in response to these efforts, terrorists and terrorist financiers have adapted, expanding and varying their methods of raising and moving funds, requiring increased innovation and vigilance by law enforcement and financial institutions.

Case Study

The September 11 hijackers used US and foreign financial institutions to hold, move and retrieve their money. They deposited money into US accounts, primarily by wire transfers and deposits of cash or traveler's checks brought from overseas. Several of them kept funds in foreign accounts that they accessed in the United States through ATM and credit card transactions. The hijackers received funds from facilitators in Germany and the United Arab Emirates as they transited Pakistan before coming to the United States. The plot cost al Qaeda somewhere in the range of $400,000–$500,000, of which approximately $300,000 passed through the hijackers' bank accounts in the United States. While in the United States, the hijackers spent money primarily for flight training, travel and living expenses.

Through reconstruction of available financial information, the US Internal Revenue Service and the US Federal Bureau of Investigation established how the hijackers responsible for the September 11 attacks received their money and how the money was moved into and out of their accounts. The 19 hijackers opened 24 domestic bank accounts at four different banks. The following financial profiles were developed from the hijackers' domestic accounts:

Account Profiles:

- Accounts were opened with cash/cash equivalents in average amounts 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 United States.
- Some of the accounts were joint accounts.
- Addresses used usually were not permanent addresses, but rather were mail boxes and were changed frequently.
- The hijackers often used the same address and telephone numbers on the accounts.
- Twelve hijackers opened accounts at the same bank.

Transaction profiles:

- Some accounts directly received and sent wire transfers of small amounts to and from foreign countries such as United Arab Emirates (UAE), Saudi Arabia and Germany.
- The hijackers made numerous attempts to withdraw cash in excess of the limit of the debit card.
- Numerous balance inquiries were made.
- After a deposit was made, withdrawals occurred immediately.
- Overall transactions were below reporting requirements.
- Funding of the accounts was by cash and overseas wire transfers.
- ATM transactions occurred with more than one hijacker present (creating a series of transactions involving several hijackers at the same ATM).
- Debit cards were used by hijackers who did not own the accounts.

International activity:

- While in the United States, 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 US Some of these traveler's checks were deposited into their US checking accounts.
- One of the hijackers received substantial funding through wire transfers into his German bank account in 1998 and 1999 from an individual.
- In 1999, this same hijacker opened an account in UAE, giving a power of attorney over the account to the same individual who had been wiring money to his German account.
- More than $100,000 was wired from the UAE account of the hijacker to the German account of the same hijacker in a 15-month period.

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

- Use of an account as a front for a person with suspected terrorist links.
- Appearance of an account holder's name on a list of suspected terrorists.
- Frequent large cash deposits in accounts of non-profit organizations.
- High volume of transactions in the account.

- Lack of a clear relationship between the banking activity and the nature of the account holder's business.

FATF suggested that, with these scenarios in mind, financial institutions pay attention to some classic indicators 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.

HOW TERRORISTS RAISE, MOVE AND STORE FUNDS

Global sanctions efforts have reduced funding to organizations from traditional state sponsors of terror leading those organizations to seek supplemental sources of income to conduct their activities.

In a December 2015 United Nations Security Council meeting, Secretary-General Ban Ki-moon told the Council, "Terrorists take advantage of weaknesses in financial and regulatory regimes to raise funds. They circumvent formal channels to avoid detection, and exploit new technologies and tools to transfer resources. They have forged destructive and very profitable links with drug and criminal syndicates — among others. And they abuse charitable causes to trick individuals to contribute. Terrorists continue to adapt their tactics and diversify their funding sources," which he noted include raising money through the oil trade, extortion, undetected cash couriers, kidnapping for ransom, trafficking of humans and arms, and racketeering.

Use of Hawala and Other Informal Value Transfer Systems

Alternative remittance systems (ARSs) or informal value transfer systems (IVTSs) that are often associated with ethnic groups from Africa, Asia and the Middle East. ARSs commonly involve the international transfer of value outside the legitimate banking system and are based on trust. The systems are referred to by different names depending upon the country: Hawala (an Arabic word meaning "change" or "transform"), Hundi (a Hindi word meaning "collect"), Chiti banking (referring to the way the system operates), Chop Shop banking (China), and Poey Kuan (Thailand).

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

Today, the process works much the same way, with people in various parts of the world using their accounts to move money internationally for third parties. In this way, deposits and withdrawals are made through hawala bankers rather than traditional financial institutions. The third parties are normally immigrants or visiting workers who send small sums to their homelands to avoid bank fees for wire transfers. Reasons for legitimate use of hawala and other IVTS include: cheaper and faster money transmission, lack of banking access in the remittance receiving country, cultural preference and lack of trust in the formal banking system. There is usually no physical movement of currency and a lack of formality with regard to verification and record-keeping. The money transfer

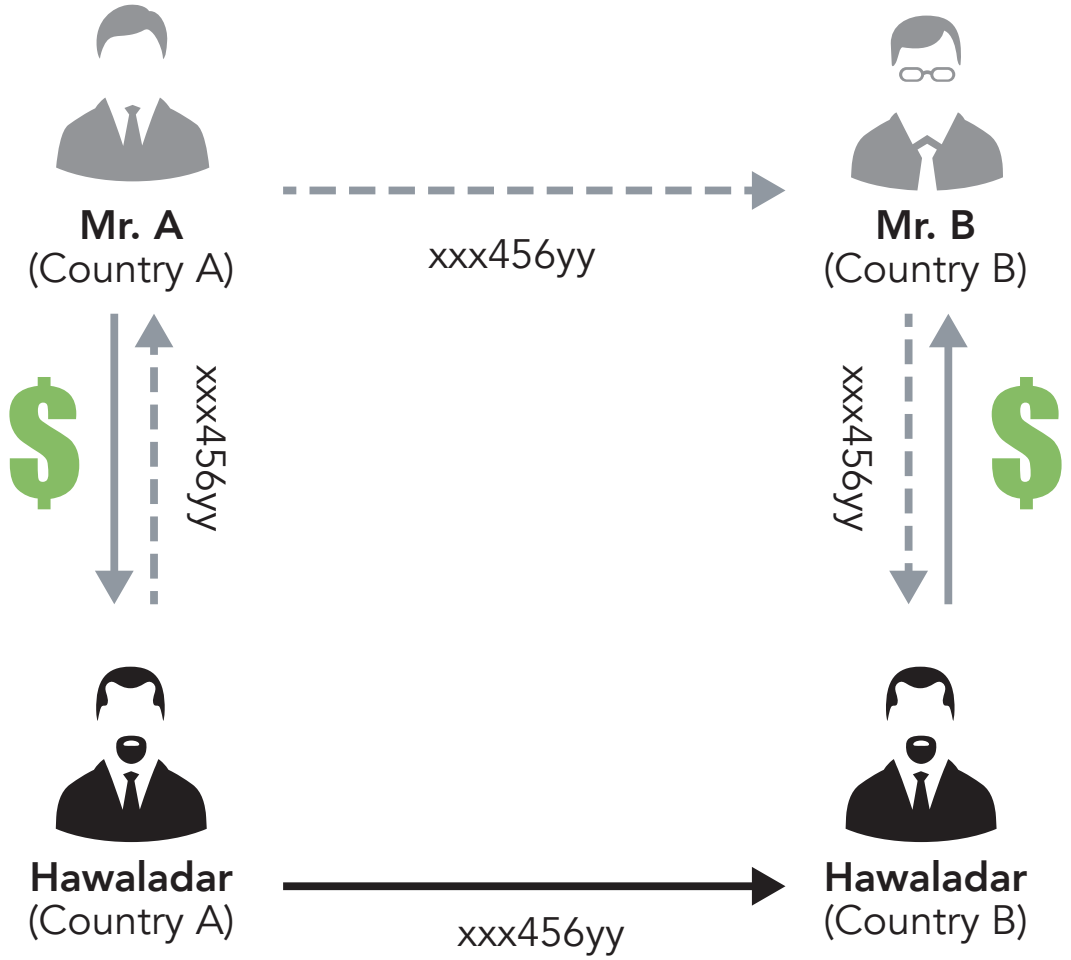
takes place by coded information that is passed through chits, couriers, letters, faxes, emails, text messages, or online chat systems, followed by some form of telecommunications confirmation. Almost any document that carries an identifiable number can be used by the receiver to pick up the values in the other country.

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. In its 2013 "The Role Of Hawala And Other Similar Service Providers In ML/TF," FATF explains that regulation and supervision of hawalas and other similar service providers remains a key challenge to authorities, also noting that as in other sectors, money laundering and terrorist financing risk increases the less regulation and supervision the hawala or similar service provider is subjected to. It is attractive for launderers because it leaves little to no paper trail as the details of the customers who will receive the funds are communicated to the receiving brokers via telephone, fax and e-mail. Recently, authorities have been observing the use of advanced internet technologies by hawala and other similar agents and suspect they are exclusively using protected online services to conduct their activities and maintain their accounts, leaving no manual accounts.

Because hawala is a remittance system, it can be used at any phase of the money laundering cycle. It can provide an effective means of placement: when the hawaladar receives cash, he can deposit the cash in bank accounts. He will justify these deposits to bank officials as the proceeds of legitimate business. He may also use some of the cash received to pay for his business expenses, reducing his need to deposit the cash into the bank account. Hawaladars often operate within or in addition to a legitimate or front business to provide cover for the activity and commingle the funds in the business accounts.

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

Hawala Transaction Example



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

Hawalas are attractive to terrorist financiers because they, unlike formal financial institutions, are not consistently subject to formal government oversight and are not required to keep detailed records in a standard form. Although some hawaladars do keep ledgers, their records are often written in idiosyncratic shorthand and are maintained only briefly. Al Qaeda moved much of its money by hawala before September 11, 2001. Al Qaeda used about a dozen trusted hawaladars who almost certainly knew of the source and purpose of the money. Al Qaeda also used unwitting hawaladars who probably strongly suspected that they were dealing with al Qaeda, but were nevertheless willing to engage in the transactions.

Case Study

On August 18, 2011, Mohammad Younis pled guilty in Manhattan federal court to operating an unlicensed money transfer business between the United States and Pakistan. One of the money transfers was used to fund the May 1, 2010, attempted car bombing in New York City's Times Square by Faisal Shahzad who is serving a life sentence in federal prison. From January to May 2010, Younis provided money transmitting services to individuals in the New York City area by assisting in the operation of a hawala. On April 10, 2010, Younis engaged in two separate hawala transactions with customers who traveled from Connecticut and New Jersey to meet with him in Long Island. In each of the transactions, Younis provided thousands of dollars in cash to the individuals at the direction of a co-conspirator in Pakistan, but without knowledge of how the customers were planning to use the funds. At no time did Younis have the license to operate a money transmitting business from either state or federal authorities. One of the individuals to whom Younis provided money was Shahzad, who on June 21, 2010, pled guilty to a ten-count indictment charging him with crimes relating to his attempt to detonate a car bomb in Times Square on May 1, 2010. During the course of his plea allocution, Shahzad acknowledged receiving a cash payment in April 2010 in the United States to fund his preparations for the May 1, 2010, attempted bombing. According to Shahzad, the April cash payment was arranged in Pakistan by associates of the Tehrik-e-Taliban, the militant extremist group based in Pakistan that trained him to make and use explosive devices. On September 15, 2010, Younis was arrested by the FBI and other agents of the New York Joint Terrorism Task Force. Younis pled guilty to one count of conducting an unlicensed money transmitting business.

Use of Charities or Non-Profit Organizations (NPOs)

After the September 11, 2001, attacks the United States government initiated the Terrorist Finance Tracking Program (TFTP) in order to identify, track and pursue terrorist groups' sources of funding. Through the TFTP, the US Government has uncovered and shut down over 40 designated charities used as potential fundraising front organizations.

Knowingly or not, charitable organizations have served as vehicles for raising and laundering funds destined for terrorism. As a result, some charities, particularly those with Muslim connections, have seen a large drop in donations or have become targets of what they claim are unfair investigations or accusations. FATF states in its 2014 Risk of Terrorist Abuse in Non-Profit Organizations (NPO): "The importance of the NPO sector to the global community cannot be overstated. It is a vibrant sector, providing innumerable services to millions of people." However, this typologies project found that more than a decade after the abuse of NPOs by terrorists and terrorist organizations was formally recognized as a concern, the terrorism threat to the sector remains, and the sector continues to be misused and exploited by terrorist organizations through a variety of means.

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

- Enjoying the public trust.
- Having access to considerable sources of funds.

- Being cash-intensive.
- Frequently having a global presence, often in or next to areas exposed to terrorist activity.
- Often being subject to little or no regulation and/or having few obstacles to their creation.

To help legitimate NPOs avoid ties to terrorist-related entities and to help them regain public trust, FATF first issued guidelines in 2002 on best practices for charities in combating the abuse of non-profit organizations. The best practices guidance was updated in 2015 with the purpose of assisting countries implement Recommendation 8 on NPOs in line with the risk-based approach; to assist NPOs mitigate terrorist-financing threats and assisting financial institutions in the proper implementation of the risk-based approach when providing financial services to NPOs.

The objective of Recommendation 8 is to ensure that NPOs are not abused by:

- Terrorist organizations posing as legitimate entities
- Exploiting legitimate entities as conduits for terrorist financing
- Concealing or obscuring the clandestine diversion of funds intended for legitimate purposes to terrorist organizations.

The best practices cover identification and mitigation of risk by countries and NPOs alike, self-regulation by NPOs, and their access to financial services. FATF recommends that NPOs:

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

FATF recommends that charities use formal bank accounts to store and transfer funds so that they are subject to the bank's regulations and controls. In turn, the banks where the accounts are established can treat NPOs like other customers, apply their know-your-customer rules and report suspicious activities.

The Charity Commission is an independent regulator of charities in England and Wales whose role is to protect the public's interest in charities and ensure that charities further their charitable purposes for the public benefit and remain independent from private, government or political interests. Their Counterterrorism Strategy Report dictates a four-strand approach to preventing abuse of charities by terrorist financiers:

- Co-operation with government regulators and law enforcement nationally and internationally.
- Raising awareness in the sector of the risks charities face from terrorism.
- Oversight and supervision through proactive monitoring of the sector in areas identified as being at higher risk.
- Intervention when abuse, or the risk of abuse, related to terrorist activity is apparent.

Case Study

In May 2013, two US women from Minnesota were sentenced in federal court for providing material support to US designated terrorist organization, al-Shabaab. Amina Farah Ali and Hawo Mohamed Hassan, naturalized US citizens from Somalia, were sentenced to 240 and 120 months, respectively, in federal prison for charges ranging from making false statements to authorities to providing material support to a terrorist organization. Evidence presented at trial proved the defendants provided support to al-Shabaab from September 2008, through July 2009. After communicating with Somalia-based members of al-Shabaab requesting financial assistance on behalf of the group, the women, along with the help of others, raised money for the terrorist organization by soliciting funds in Somali neighborhoods in Minnesota and other cities in the US and Canada. Funds were often sought under false pretenses, leading those who donated to believe they were helping the less fortunate. Funds in direct support of al-Shabaab were obtained by the defendants through participation in teleconferences that featured speakers who encouraged listeners to make donations. Once they received the funds, Ali and others utilized multiple remittance services for in excess of twelve fund transfers using false recipient names to conceal the true intended beneficiary, al-Shabaab.

Case Study

The Holy Land Foundation (HLF) was an Islamic charitable organization operating multiple locations in the United States and based out of Richardson, Texas. HLF was shut down by the US Treasury in 2001 and designated for its support of US-designated foreign terrorist organization, Hamas. This support consisted of direct fund transfers to HLF offices in the West Bank and Gaza affiliated with Hamas, and transfers of funds to Islamic charity committees and other charitable organizations that are part of Hamas or controlled by its members. HLF and five of its leaders were convicted in November 2008 by the US Government on charges of providing material support for terrorism. A similar organization, International Relief Fund for the Afflicted and Needy-Canada (IRFAN-Canada), was identified and declared a terrorist entity in April 2014 by Public Safety Canada under the Criminal Code. The Canadian government alleged that, between 2005 and 2009, the group funneled $14.6 million to Hamas. It has also been alleged that those funds originated in part from HLF and were subsequently transferred to a UK-based non-profit organization, which in turn routed the funds to several Palestinian aid organizations in Gaza and the West Bank known to be under the control of Hamas or its leaders. Both HLF and IRFAN-Canada are believed to have been created solely for the purpose of raising support, financial and otherwise, for Hamas.

Emerging Risks for Terrorist Financing

The FATF's 2015 Emerging Terrorist Financing Risks details rising threats as:

- **Self-funding by FTFs**

  The advent of social media, smartphone applications, and internet sharing sites now provide terrorist organizations global reach at little to no cost. Foreign terrorist fighters (FTFs) and terrorist sympathizers can self-radicalize and/or communicate with terrorist organizations like never before. The often low cost associated with perpetrating a terrorist act on a "soft target"

(i.e., a civilian, non-military target that is relatively unprotected and thus vulnerable to terrorist attacks) means such acts can be self-funded. Self-funding includes sources such as employment income, social assistance, family support, and bank loans, which makes detection nearly impossible without the association of other aggravating terrorist financing indicators.

FBI Director James Comey stated at a US Senate Judiciary Hearing on December 9, 2015, "Terrorists, in ungoverned spaces, disseminate poisonous propaganda and training materials to attract troubled souls around the world to their cause. They encourage these individuals to travel, but if they cannot travel, they motivate them to act at home. This is a significant change from a decade ago."

Case Study

On December 2, 2015, in San Bernardino, California, Syed Rizwan Farook and his wife, Tashfeen Malik, opened fire on his co-workers at a party, killing 14 people and injuring 22. The couple was subsequently killed during a shootout with police. Federal authorities have said Farook spent years becoming more radicalized and violence-oriented, in part by watching videos that advocated jihad. On the day of the attack, a Facebook account used by his wife posted a pledge of allegiance to the terror group ISIS (Islamic State in Syria). This attack was consistent with the profile for many terrorist acts in that it appears to have required a low total dollar amount to carry out. Farook was employed by the State of California as a Health Inspector, providing him a source of income with which to obtain some of the weapons used in the commission of the act (a straw purchaser was used to obtain the weapons). He received additional funding through a $28,500 loan provided by an online peer-to-peer lender that matches investors with borrowers. No specific indicators were identified that would have alerted the lender to the shooter's intentions and by all accounts his employment profile and creditworthiness provided sufficient reason to complete the loan.

- **Raising Funds through the use of Social Media**

  Social media has created the ability to build social and information-sharing networks like never before in human history. This incredible advance in technology presents a unique opportunity for terrorist organizations to communicate and raise money for their causes, and the potential to reach into every home in every country in near real time. Crowdfunding and sharing of virtual or prepaid account information are a few of the methods through which social media has been leveraged by terrorists. This presents unique difficulties for law enforcement not only due to the increased dispersion of the activity but also the need for cooperation from both financial institutions and social media platforms.

  Case Study

  An example of an individual raising funds through social media is Shafi Sultan Mohammad al-Ajmi, designated by the US Treasury in August 2014 as a supporter of terrorists in Syria and Iraq. Al-Ajmi operates regular social media campaigns seeking donations for Syrian fighters and is one of the most active Kuwaiti fundraisers for Al Nusrah Front (ANF). Al-Ajmi publicly admitted that he collected money under the auspices of charity and delivered the funds in person to ANF and acknowledged purchasing and smuggling arms on behalf of ANF.

- **New Payment Products and Services** *(See Risks Associated with New Payment Products and Services)*
- **Exploitation of Natural Resources**

  Terrorist organizations that hold or maintain control over territory or operate in a country with poor governmental control of the territory may take control of natural resources such as gas, oil, timber, diamonds, gold (and other precious metals), wildlife (e.g., ivory trading), and historical artifacts, or extort companies that extract those resources to both fund terrorist acts and support day-to-day activities. These resources themselves may be sold on the black market or to complicit companies where they can then be integrated into the global trade sector. An awareness of geographies where terrorist organizations operate or maintain control, current commodity prices, and strong multi-jurisdictional partnerships are necessary to combat this method of terrorist funding which has the potential to generate vast sums.

NOTES: