CHAPTER 4

COMPLEX FRAUDS AND FINANCIAL CRIMES

LEARNING OBJECTIVES

After completing this chapter, you should be able to:

4-1 Differentiate between a predator and an “accidental fraudster.”
4-2 Explain why collusion poses unique prevention and detection challenges.
4-3 Describe how the concept of an “organization” is involved in mixing illegal activities with legitimate ones.
4-4 Explain the difference between “following the money” and “tracing the money.”
4-5 Discuss why financial statement fraud is often considered a complex fraud.
4-6 List different types of schemes associated with complex frauds.
4-7 Contrast the objectives of terrorists and organized criminals.
4-8 Identify and describe the different types of banks.
4-9 Explain the difference between tax avoidance and tax evasion.
4-10 List and discuss some of the more common securities fraud schemes.

CRITICAL THINKING EXERCISE

A woman came home with a bag of groceries, got the mail, and walked into the house. On the way to the kitchen, she walked through the living room. In the living room, she glanced in her husband’s direction. Sadly, her husband had blown his brains out. She then continued to the kitchen, put away the groceries and made dinner.

What might explain this behavior?

“PREDATORS” VERSUS THE “ACCIDENTAL FRAUDSTER”

The common fraudster is usually depicted with the following characteristics: first-time offender, middle-aged, male, well educated, married with children, trusted employee, in a position of responsibility, and possibly considered a “good citizen” through works in the community or through a church organization. This individual is often described as having some nonsharable problem, typically financial in nature or that the problem can only be solved with money, which creates the perceived pressure. When aligned with opportunity and the ability to rationalize his or her actions, the otherwise good citizen succumbs to pressure, develops one or more fraud schemes and misappropriates assets or commits an act involving some form of corruption. This person might be characterized as the “accidental fraudster.”

Not withstanding the fraud act, the accidental fraudster is considered a good, law-abiding person, who under normal circumstances would never consider theft, breaking important laws, or harming others. When discovered, family members, fellow employees, and other persons in the community are often surprised or even shocked by the alleged behavior of the perpetrator. Because many of these perpetrators are in positions of trust (which creates opportunity), well educated, and have leadership-level employment, Edwin H. Sutherland, in 1939 described them as “white-collar criminals.”

White-collar crime, as designated by Sutherland, is crime in the upper, white-collar class, which is composed of respectable or respected business and professional men (and now, almost as often as not, women). White-collar crime is also referred to as occupational fraud or economic crime. The white-collar criminal’s actions are consistent with the notion of a trust violator, and the crime is typically associated with an abuse of power. Despite some shortcomings with this type of descriptive terminology, white-collar
prior employers had prosecuted Mr. Woods. The choice made by each of his former employers allowed quietly terminated Mr. Woods. It's possible that Christopher Woods might be alive today if any of the Woods had perpetrated a fraud. In the prior three incidents, upon discovery, the previous employer had missing funds. What the employer did not know is that the current incident was the fourth time that Mr. any public disclosures of the fraud incident provided that Mr. Woods reimburse the company for the collecting additional insurance proceeds related to the home structure and contents. All of this was to repay his most recent former employer as restitution for a fraud that he had been perpetrating.

Mr. Woods’ most recent employer had agreed to desist from filing charges against him or making any public disclosures of the fraud incident provided that Mr. Woods reimburse the company for the missing funds. What the employer did not know is that the current incident was the fourth time that Mr. Woods had perpetrated a fraud. In the prior three incidents, upon discovery, the previous employer had quietly terminated Mr. Woods. It’s possible that Christopher Woods might be alive today if any of the prior employers had prosecuted Mr. Woods. The choice made by each of his former employers allowed him to quietly move on to his next victim.

Mr. Woods is not an accidental fraudster; he is a predator. The predator seeks out organizations where he or she can start to scheme almost immediately upon being hired. At some point, many accidental fraudsters, if not caught early on, move from behavior characterized by the description of an accidental fraudster to that of a predator. Financial statement fraud perpetrators often appear to start as accidental fraudsters or even as managers of earnings and, sooner or later, become predators.

Beyond the predator-type person who seeks to deliberately defraud organizations with seemingly little remorse, we also find individuals and organizations that have operational modus operandi where a complex fraud or financial crime is inherently part of their goals and objectives. Organizational crimes occur when public and private companies, nonprofits, and government entities, otherwise legitimate and law-abiding organizations, are involved in a pattern of criminal activity. Corporate violations include administrative violations that involve noncompliance with agency, regulatory, and legal requirements. In other cases, organizations are deliberately established with at least some nefarious purposes in mind. We often think about organized crime, drug trafficking, and terrorism financing for the more complex frauds and financial crimes involving organizations. Organized criminal activities often involve many individuals, organizations, shell companies, and cross-jurisdictional borders. Some of the crimes that are typically observed include conspiracy and RICO (Racketeer Influenced and Corrupt Organizations) Act violations, money laundering, and mail and wire fraud. With terrorism financing, illegal acts derived from the USA Patriot Act come into play.

The important point is that predators and organizations focused on criminal activities exist and that reference to these types of entities as predators helps us to better understand their activities and motives in order to better investigate allegations of fraud and financial crimes. Typically, these types of entities are involved in complex frauds, corruption schemes, and financial crimes. Because their activities are far more deliberate from the outset than those of the accidental fraudster, they are better organized, have better concealment schemes, and are better prepared to deal with auditors and other oversight mechanisms. The concern is that in many cases the fraud triangle may not apply to the predator. Nevertheless, the primary investigative approach that focuses on the elements of fraud and adheres to evidence-based decision making holds quite well. Investigations centered on the act (the complex fraud or financial crime), the concealment of the crime, and the conversion (the personal benefit derived by the perpetrator from his actions) will lead to the development of a solid case from which the judicial community may determine the best course of remediation. Complex fraud and financial crime schemes include the following: money laundering
associated with organized criminal activities, terrorism financing, money flows associated with drug trafficking, tax evasion, deliberate misrepresentation of an entity’s financial performance, and deliberate bankruptcy misreporting. Violations arising from these schemes may include money laundering, corruption, tax fraud, financial statement fraud, conspiracy, and mail and wire fraud.

COLLUSION: MULTIPLE INDIVIDUALS, ORGANIZATIONS, AND JURISDICTIONS

One of the central elements to complex frauds and financial crimes is that of collusion. Collusion may be among individuals within an organization, individuals across organizations, and multiple organizations. Collusion often spans multiple jurisdictions, including local, state, federal, and international boundaries and related laws. ACFE’s report to the nation indicates that when collusion is involved, dollar amounts associated with fraud losses increase dramatically. The losses caused by individual predators can be substantial, but when those individuals work in concert with others, the damage can be devastating and far more pervasive.

The primary concern when collusion is involved is that internal controls are generally ineffective in preventing fraud and other financial crimes. The primary internal control of segregation of duties helps to ensure that no individual controls every aspect of a transaction and separates the custody, accounting, and approval functions. Internal controls also include independent checks on performance and assurance of compliance with applicable laws and regulations. While internal controls cannot prevent collusive fraud and financial crimes, they may assist in the detection of such activities. In particular, independent monitoring may reveal that internal controls have been circumvented through collusion.

If the predators are organized around criminal activities, however, it is unlikely that monitoring will have any impact because part of the goals and objectives of an illicit organization is to disguise the nature of its real operations from outsiders, including auditors, regulators, and law enforcement. Persons inside the organization, across organizations, and across jurisdictions act in such a manner so that the true underlying nature of the organization and its activities cannot be discovered.

LEGITIMATE ACTIVITIES MIXED WITH ILLEGAL ACTIVITIES AND THE NEED TO ISOLATE ILLEGAL ACTIVITIES

Another element of complex frauds and financial crimes is that the perpetrators often mix legitimate business activities with their unlawful transactions. Money laundering provides an excellent example of a complex financial crime that is designed to mix monies from some legitimate and legal activity with proceeds obtained through some illegal activity. Understanding the essence of complex frauds and financial crimes requires attention to the definition of “the organization.” Using the crime of money laundering as an example, assume that a local neighborhood tavern is used as a conduit for this activity. The operations of the tavern may be completely legitimate, except for the money laundering activity. The tavern is also part of a greater organization in which other persons and/or entities are transacting illegal business activities that generate illicit cash proceeds. This cash needs to be “laundered” to appear legitimate.

To understand the motivation of the tavern’s owner, we refer to the M.I.C.E acronym: the motivation could be money, ideology, coercion, or ego. While it is unlikely that the tavern owner would get involved in an illegal money laundering operation to satiate his ego, they may be willing to play a role to obtain a “piece of the action” (money), to further a cause in which they believe (e.g., to fund terror operations) or because they are being threatened (coerced). Examples of coercion could be threats of physical harm to the owner, patrons of the tavern, the owner’s family, or the physical premises of the tavern. Investigators must also have some sense of the entire story: who, what, when, where, how, and why (if known). To attempt to prosecute the tavern owner without a sense of the greater story will be far more difficult because the investigator will be unable to communicate that understanding to prosecutors, defense attorneys, judges, and jurors. To tell a more complete story, fraud and forensic accounting professionals must know the greater “organization,” even if the organization is not recognized as a legal entity.

Inherently, most complex fraud and financial crime schemes include a mixture of legitimate and illicit activities. One of the main challenges for investigators is to isolate the illicit from the legitimate activities. This is an essential element for successful remediation of the crime and can be accomplished by using the investigative tools and techniques highlighted in this textbook.
ASSET FORFEITURE AND SEIZURE AND DISMANTLING ORGANIZATIONS

Asset forfeiture or seizure is an important part of the process of dismantling an organization, particularly with complex frauds or financial crimes. As discussed above, the nature of the activities is such that collusion is likely involved. In more serious cases, the underlying design, goals, and objectives constitute illegal activities. By seizing assets, the perpetrators are being punished and the organization is dismantled to make it more difficult for another person in the chain of command to take over the remaining operations.

First, money and other assets must be identified during the investigative process. The investigation needs to show that the perpetrator(s) or the organization(s) involved received assets and what happened to those assets. This requires that all records—banking, public, business, personal, financial, and nonfinancial—are searched to identify assets available for seizure, and to help separate those related to illegal activities from those generated from legitimate sources. This is accomplished through a process of “following” or “tracing” the money. Chapter 15 discusses this process in detail.

Dismantling the organization by seizing operational assets, confiscating cash, and freezing funds is an effective tool for forensic professionals in the pursuit of their responsibilities. Criminal organizations, drug traffickers, and terrorists need money to achieve their goals because they must cover operating costs, including paying employees, investing in infrastructure, paying legal fees, and covering other costs comparable to those of a legitimate business enterprise. While criminal organizations cannot declare bankruptcy, the seizure of assets can have the effect of putting them out of business, at least for the short term.

SCHEMES AND ILLEGAL ACTS ASSOCIATED WITH COMPLEX FRAUDS AND FINANCIAL CRIMES

As noted above, the profile of perpetrators of complex frauds and financial crimes tends to align more with those of predators rather than the accidental fraudster. Their motivation and intent is generally more nefarious and deliberate, and their mode of operation more sophisticated. Furthermore, the perpetrators of complex frauds and financial crimes often collude with others who can provide additional resources or legitimacy for their activities.

Financial statement fraud is more often than not a complex fraud. It almost always involves the chief financial officer, controller, or some other sophisticated participant within the financial reporting structure. It also often involves top leadership in the organization such as the chief executive officer, chief operating officer, president, or others with significant levels of authority. While not always predatory, at least at the time of inception, it is almost always collusive. Executive-level individuals work in concert (collusively) to override the system of internal controls through the sophisticated use of journal entries, significant estimates, and other financial reporting choices, and through material, unusual, one-time transactions. Due to the unique nature of financial statement fraud, the large dollars involved, its impact on stakeholders, and its connection with the audit profession, it is addressed separately in Chapter 14.

Similarly, corruption schemes are addressed in Chapter 13. Corruption includes bribery, illegal gratuities, economic extortion, and conflicts of interest. Corruption is collusive by its very nature and tends to be predatory. At least one party, and possibly all parties, to the corruption scheme set out to achieve certain goals as a result of their activities. While illegal gratuities and conflicts of interest may fall close to being ethically questionable, specific laws make such activities illegal.

When one thinks of organized criminals, drug traffickers, and terrorists and their financiers, one typically thinks of strong organizations and carefully planned operational activities. These types of organizations are sophisticated and tend to be very disciplined. Furthermore, they tend to make extensive use of technology. The advent of disposable cell phones, Internet money transfers, and beaming (infrared) cell phone technology, the easy movement of money around the world, and banking and legal jurisdictions committed to secrecy and privacy have made tracking these types of criminals and their activities (financial and nonfinancial) challenging for those saddled with the responsibility of policing them and stopping such activities.

Organized Crime

The definition of organized crime is a hotly debated subject. The Organized Crime Control Act of 1970 defines the activity as “The unlawful activities of . . . a highly organized, disciplined association.” The traditional understanding is that organized crime or criminal organizations are entities controlled and
operated by criminals for the common purpose of generating positive cash flows from illegal acts. The term “organized” is central to the definition. Many of these organizations are professionally run as if they were a traditional for-profit business. Their operations include hiring (firing), training, mentoring, information systems, a hierarchical structure, and other attributes associated with effective and efficient business entities. As such, the organizations are opportunistic, diversified, and require political support (legal or otherwise) and capital investment. Racketeering is the act of engaging in criminal activity as a structured group, and organized criminal organizations are often prosecuted under RICO.

Most people think of the Italian Mafia (as portrayed in the film The Godfather), Al Capone, and similar images when organized crime is mentioned. Organized crime, however, is far more global and complex than these traditional images suggest. Organized crime can be found in even the tiniest and most remote regions of the world. Some of the more recognized organized crime activities in recent times include the rise of the Russian mob in the wake of the collapse of the Soviet Union, organized criminals from Africa who specialize in narcotics and financial scams, Asian crime organizations grounded in secret societies, and crime groups located in former Eastern Bloc countries. The FBI estimates the annual impact of organized crime profits to be approximately $1 trillion. Organized crime, when the opportunity presents itself, will manipulate and monopolize financial markets, particularly those in less developed areas; infiltrate labor unions; align itself with traditional businesses, such as construction and trash hauling; engage in the purchase of political support through bribery, extortion, blackmail, intimidation, and murder; as well as organize and carry out various financial frauds.

The more famous criminal enterprises are those associated with the Italian Mafia. Italian organized crime consists primarily of four major groups, estimated to have 25,000 members and more than 250,000 affiliates worldwide. In recent years, the Italian mob has collaborated with other criminal organizations. The Italian groups have been involved in heroin smuggling for decades, as well as money laundering activities. In addition to narcotics, the Italian mob, earning as much as $100 million annually, has been involved in bombings, counterfeiting, fraud, illegal gambling, kidnapping, murder, political corruption, and the infiltration of legitimate business. The four major organizations that make up the Italian mob consist of the Sicilian Mafia, the Camorra or Neapolitan Mafia, the Ndrangheta or Calabrian Mafia, and the Sacra Corona Unita or United Sacred Crown.

In the United States, the FBI is most concerned about La Cosa Nostra (LCN). The literal translation of La Cosa Nostra is “this thing of ours.” LCN consists of several aligned family organizations and cooperates with the four groups identified above who operate out of Italy. LCN is involved in a multitude of criminal acts including corruption, drug trafficking, illegal gambling, infiltration of legitimate business, labor racketeering, loan sharking, murder, stock manipulation, and tax fraud. Labor racketeering has been a significant source of LCNs national profit, power, and influence.

Balkan organized criminal enterprises are associated with Albania, Bosnia-Herzegovina, Croatia, Kosovo, Macedonia, Serbia, Montenegro, Bulgaria, Greece, and Romania. The groups from these areas arose from their traditional protection and support needs that were provided for by various clans. Over time, these clans morphed into organizations entrenched in organized crime. Many of these countries were under the control of the Soviet Union until its collapse. At that time, these groups, which had been working in the black market, infiltrated and exploited the new democratic governing bodies. These groups are not as well organized as others, still holding to their clan roots, but are involved in fraud, gambling, money laundering, drug trafficking, human smuggling, robbery, murder, and other violence.

Asian crime groups grew out of triads, tongs, and street gangs. These groups arise from, and operate in, Asian countries such as China, Japan, Korea, Thailand, the Philippines, Cambodia, Laos, and Vietnam. The groups from China predominantly arose from triads or underground societies. In contrast, the organizational structure of the groups from the remaining countries were influenced by tongs, triad affiliates, and street gangs. These groups tend to commingle legal and illegal activities. The illegal activities often include extortion, murder, kidnapping, illegal gambling, prostitution, loan sharking, human trafficking, drug trafficking, theft of intellectual property, counterfeit computer, textile, and other products, money laundering, and financial fraud.

Eurasian criminal enterprises grew out of the Soviet prison system, emigrated to the West, and proliferated in the former Soviet Union after its collapse. Eurasians specialize in sophisticated fraud schemes, tax evasion, and public corruption. The activities of the Eurasian groups have destabilized the governments of the former Soviet Union. A major concern is the access of these groups to leftover Soviet nuclear weapons. Some of the fraud schemes include those associated with healthcare, auto insurance, securities and investment fraud, money laundering, human smuggling, prostitution, drug trafficking, auto theft, and the transportation of stolen goods.
African organized crime is most known for its efforts with illegal drug trafficking and online financial frauds. Nigeria is known as one of the hubs for organized crime enterprises in Africa. Other locales for organized criminals include Ghana and Liberia. Nigerian organized crime is famous for its financial frauds, which the FBI estimates cost Americans $1 billion to $2 billion annually. Some of the criminal activities include auto insurance fraud, healthcare billing fraud, life insurance scams, bank, check, and credit card fraud, as well as other sophisticated fraud schemes.

Middle Eastern crime groups are engaged in a variety of criminal acts including money laundering, cigarette smuggling, and identity theft. Generally, these groups are for-profit enterprises and are not overtly affiliated with terrorist groups such as Al Qaeda. Like the Balkan groups, these organized criminal groups are less well organized, and their affiliations tend to be based on tribal and family associations. These groups are known to be involved in auto theft, financial fraud, interstate transportation of stolen items, drug trafficking, document fraud, healthcare fraud, identity theft, cigarette smuggling, and the theft of baby formula for the purposes of cutting drugs.

Organized crime, including drug trafficking as discussed below, is investigated using traditional techniques such as undercover operations, surveillance, wire tapping, confidential informants, victim interviews and testimony, document review and analysis, examination of public records, and following the money (direct, indirect, and ad hoc financial analyses). With the exception of terrorists, the primary motivation of organized criminals is the ability to make more money through collaboration than when working alone or in smaller, less organized, and less disciplined groups. The flow of money, along with an understanding of the rest of the story line (how, what, when, where, how, and why), provides a solid investigative approach for case development.

**Drug Trafficking**

Drug trafficking is a specific example of an organized criminal organization. The primary difference is that these organizations specialize in trafficking narcotics for illegal sale in countries all over the world. Mexican drug traffickers have a significant market share of illegal drugs transported into the United States, including cocaine, marijuana, heroin, and methamphetamine. In recent years, the Mexican traffickers have become more professional and violent. Due to the significant profits associated with illegal drugs, drug producers, traffickers, and distributors are more likely to collaborate. Around the world, the United States and other nations forge partnerships to address the various problems associated with illegal drugs.

According to Drug-Free America, illegal drug trafficking costs the United States $70 billion annually. Mexican transporters exploit the 2,000-mile shared border between the United States and Mexico as the entry point for the majority of illegal drugs into America. During 2000, 89 million automobiles, 4.5 million trucks, and 293 million people entered the United States from Mexico.1 In addition to border crossings, drug traffickers also utilize airplanes, high-speed boats, and cargo ships entering and exiting U.S. waters. The Drug Enforcement Agency (DEA) estimated in 2000 that 50 percent of the cocaine entering the United States, and 85 percent of methamphetamines, entered from Mexico.

Mexican traffickers are organized, have the skills necessary to be effective, and demonstrate high levels of professionalism. Some of the Mexican trafficking organizations include the Juarez Cartel, Arellano-Felix Brothers’ organization, the Caro-Quintero organization, and the Amezcua-Contreras organization, all of which control the Tijuana and Ciudad Juarez areas around the Gulf of Mexico. These groups have loosely organized themselves as the Federation. The partnership provides greater security and profitability to the membership. These groups are estimated to earn tens of billions of dollars annually.2 The Mexican organizations appear to be more specialized (drug manufacturing and transportation, related money laundering, and unrelated robbery) than most organized criminal groups, which tend to be more opportunistic and engage in broader ranges of illegal activity.

Although the groups are not known for their violence within the borders of the United States, outside of the United States they have been known for corrupting and killing law enforcement and public officials who threaten their livelihood. Within the United States, their efforts are more directed to corruption, including massive bribes. These bribes, for example $50,000 for allowing one vehicle to cross the border unimpeded, are concentrated at the point of entry because once in the United States, the probabilities of being detected drop considerably until the illegal drugs are sold to end users. These groups are considered to be professionally operated with centralized decision making. While these groups are known for trafficking, they do not distribute the narcotics once the drugs are inside the United States. Most of that part of the operation is handled by organized criminal organizations rooted in Dominica and Columbia.
CHAPTER 4 COMPLEX FRAUDS AND FINANCIAL CRIMES

These groups are considered highly professional. The narcotics transfers from the traffickers to the distributors are carefully orchestrated and often include surveillance of local law enforcement anti-drug units to ensure that the transfers will not be disrupted. Like the bootleggers of Al Capone’s time, the traffickers will also partner with legitimate cargo carriers and conceal the narcotics among legal goods. Traffickers also exploit the advances in technology by communicating over the Internet, using various forms of encryption as well as more traditional communications via fax, phone, and pagers. The sophisticated groups also employ accountants, lawyers, and other professionals that are necessary to conduct their operations. Mexican criminal organizations are not alone in the global efforts to supply drugs. Almost all organized crime groups from around the world including those from Asia, Eurasia, the Balkans, Africa, the Middle East, and the former Soviet Union are participants in drug manufacture, transportation, and distribution to some degree.

Recommendations for effectively attacking the drug trafficking problem in the United States include the following:

- Improving coordination among U.S. drug fighting agencies
- Strengthening the legal institutions in Mexico and other countries where drugs are produced and transported, including the development of effective and respected law enforcement, prosecution, and judicial systems that address both the illegal acts and the associated corruption
- Improving multilateral coordination between the United States and other nations involved in counter-narcotics efforts
- Continuing and expanding programs that emphasize demand reduction in the United States and other countries with large numbers of narcotics users

In short, bilateral and multilateral counter-narcotics efforts are the key effective responses to fighting drug trafficking. Only with coordinated and sustained efforts, including those centered on information and intelligence sharing, will law enforcement worldwide be able to successfully combat illegal drugs.

Terrorism Financing

Even before September 11, 2001, the United States faced unprecedented challenges in this area. Terrorists, determined to undermine our way of life, made security a primary concern for government entities such as the CIA and Department of Defense. Because terror organizations need funds to operate and purchase guns, explosives, and other supplies; require training; and often function loosely or efficiently as organizations; fraud professionals and forensic accountants are integral to following and tracing their funding sources. The goal of fraud examiners and financial forensic professionals is to deny terrorist groups access to the international banking system. This has the affect of impairing their ability to raise funds, thus exposing, isolating, and incapacitating their financial networks.

Terrorism, as its main objective, is designed to intimidate a population or to compel a government to do or abstain from doing any act. Terrorists attempt to intimidate or coerce persons, governments, and civilian populations through the use of force or violence, real or threatened, to achieve political or social objectives. While drug traffickers and organized criminals are organized around deriving financial gain from their activities, terror groups’ objectives are publicity, legitimacy, and influence. Like all entities, however, terrorist groups must build and maintain infrastructure and operations to achieve their objectives. Money is required to attract and retain personnel, to support their activities, and to pay for training facilities, firearms, explosives, media campaigns, political influence, and even to support social projects such as schools and hospitals in order to further their ideological objectives. Terrorists often live modestly, a characteristic in contrast with that of drug traffickers and organized criminals. Although the international banking system is required for successful terrorist activities, funding requirements for the organization may be relatively small by comparison. The small nature of the transactions makes the investigation similar to looking for a needle in a haystack.

Two primary sources of terrorist financing are state sponsorship and revenue generating from legitimate and illegitimate activities. Iran, North Korea, Syria, and others are often denoted as state sponsors of terrorism. Each of these countries, for differing reasons, awards resources to active terrorist organizations. Due to bank secrecy laws and other impediments to transparent financial transactions, the Cook Islands, Dominica, Egypt, Grenada, Guatemala, Hungary, Indonesia, Israel, Lebanon, the Marshall Islands, Myanmar, Nauru, Nigeria, Niue, Philippines, Russia, St. Kitts and Nevis, St. Vincent, the Grenadines, and the Ukraine are considered places where terrorists may find some safety. In a post-9/11 world, these countries
appear to have improved their efforts to assist international law enforcement in tracking and prosecuting criminals. Nevertheless, their laws do not afford the reporting requirements and financial reporting transparency commonly found within the United States.

Osama bin Laden, leader of the al-Qaeda terrorist network, is one of fifty-three children of a Saudi construction magnate. He inherited the foundations for his fortune, which is estimated at $5 billion. Beyond his inheritance, Osama bin Laden has invested in legitimate companies including a bakery, a furniture company, and a cattle-breeding operation. Osama Bin Laden is an example of an individual sponsor of terror, whereas his legitimate business operations are organizational examples.

Charities may be an additional source of terrorist funding. Examples include the Holy Land Foundation in Texas (now disbanded), and the Al-Aqsa Foundation in Germany. Each of these has been investigated for funneling donations to terrorists. In many cases, the donors to these “charities” do not know that they are funding terrorist activity.

Terrorists also obtain funds from both legitimate and illegitimate revenue generating activities; by mixing funding from legal business activities and unlawful acts, terrorist organizations appear similar to other criminal organizations. Related to criminal behavior, terror organizations support themselves with kidnapping, extortion, and protection money. For example, terrorist organizations such as FARC (Revolutionary Armed Forces of Columbia) and the AUC (United Self-Defense Forces of Columbia) in Colombia, are characterized by the kidnapping of both governmental and nongovernmental persons for ransom. FARC and AUC also enforce the payment of “taxes” on cocaine production. Criminal activities by terror organizations have been observed in the United States and include large-scale identity theft, smuggling, fraud, theft, robbery, and narcotics trafficking. Consistent with other criminal organizations, funds from legitimate sources are commingled with those from illegitimate sources. Legitimate sources of income may include donations, membership dues, sale of publications, cultural and social events, and solicitations and appeals to wealthy individuals with similar ideological beliefs.

When a criminal activity generates income, like other criminal organizations, terror groups must find a way to position the money for its intended use without attracting attention to the terrorist organization, the persons involved, or the underlying unlawful behaviors. Criminals do this by money laundering: disguising the sources, changing the form, and moving the funds to places where they are less likely to attract attention. In addition, terrorist groups have been known to utilize less restrictive overseas banks, to use informal banking systems such as Hawala, to smuggle cash, to structure banking transactions to sufficiently small amounts, and to use travelers’ checks and money orders.

Countries like the United States attempt to monitor and track terrorists and their supporting organizations on several fronts, including the monitoring of financial transactions. Similar to the fraud triangle for the accidental fraudster, the “terrorism triangle” is necessary as a precursor set of conditions for terrorism activities to exist. Terrorists and their related activities exist only under the conditions of opportunity, ideological motivation (versus pressure), and ideological rationalization. Inherently, terrorists have the ideological motivation to inflict terror; similarly, most terrorists show little remorse and rationalize their activities based on their ideological beliefs. This observation is true not only for al-Qaeda, but also for Timothy McVeigh and Ted Kaczynski, the Unabomber. Opportunity may be the most important attribute for investigators because without the opportunity to generate, move, and control cash flows, the financing of terror cannot occur.

The elements of fraud provide a solid structure to investigate attempts at terror financing and to identify illegal financial activities associated with terror: the act, the concealment, and the conversion. First, the terrorist financier must commit an illegal financial or fraud act, for example, identity theft. Knowing that an illegal act has taken place and tracing the funds associated with the act back to the perpetrator is a traditional investigative tactic. Secondly, terrorists and their sponsoring organizations must conceal their illegal activities so that no one knows the act has taken place, or if the act is discovered, the act cannot be traced to terror. Finally, the perpetrator needs to obtain benefit (conversion) from committing the act. In the case of the terrorists, the funds must become available for unrestricted use to attract and retain the knowledge, skills, and abilities required to carry out terror acts. Like traditional fraud detection activities, fraud professionals and forensic accountant need to be observant, searching for accounting anomalies, internal control weaknesses, and lifestyle symptoms such as:

1. Movement of funds through the Cook Islands, Dominica, Egypt, Grenada, Guatemala, Hungary, Indonesia, Israel, Lebanon, Marshall Islands, Myanmar, Nauru, Nigeria, Niue, Philippines, Russia, St. Kitts and Nevis, St. Vincent and the Grenadines, and Ukraine.
2. Money flowing to foreign beneficiaries located in Persian Gulf States, particularly those known for state-sponsored terrorism.

3. The use of wire transfers for business activities that would not normally generate the wire transfer activity.

4. Financial activities inconsistent with the stated purpose of the business.

5. Financial activities not commensurate with the stated occupation of the individual.

6. The use of multiple accounts at a single bank with no apparent legitimate purpose.

7. Use of high-dollar currency and travelers’ checks not commensurate with the business’s purpose, or the individual’s lifestyle or occupation.

8. The structuring of deposits at multiple branches of the same bank to avoid CTR (currency transaction reporting) requirements.

9. The use of false identities, documents, or “straw men.”

10. Exploiting the privacy and secrecy benefits of sympathetic international jurisdictions.

Money Laundering

Money laundering is the disguising of the existence, nature, source, ownership, location, and/or the disposition of assets derived from criminal activity. More simply, money laundering is a process to make dirty money appear clean. The world is a smaller place due to technology and travel options. People and assets can move all over the world at almost any time with minimal legal restrictions, moving by air, land, and sea. Money, communications, and information can move even easier by traveling inside small fiber optic cables as pulses of electricity.

Fundamental to understanding money laundering is the need to define money. Money is “anything of value” that can be easily transferred from person to person and is such that most persons would accept it as an item of value or as a form of payment for goods, services, and debts owed. Money, or at least the concept of money as it applies to money laundering, can be currency, diamonds, gold, credit cards, money orders, stocks, bonds, cashier’s checks, rare coins, wire transfers, gift cards, prepaid phone cards, debit cards, prepaid credit cards, etc. As long as it has value, is considered an acceptable form of payment, and is transferable among participants for a transaction it can be characterized as money.

The process of money laundering relies upon movement and takes place in three distinct stages:

Placement: The initial stage of money laundering involves placing it into the financial system. This stage requires some mechanism or vehicle for getting the money into the financial system without being noticed. At least three general methods are available for placement:

1. A cash-based or cash-heavy business can be integral to the placement stage of money laundering. Banks and other financial institutions are used to receiving large sums of cash from cash-based businesses. Restaurants, bars, laundromats, nightclubs, vending machine businesses, and check cashing businesses, as examples, operate with large amounts of cash and can be used as a means to place cash into the financial system through periodic deposits.

2. Structuring of cash deposits to fall under federal reporting guidelines can be a means of placing cash into the financial systems. Federal standards require that any cash deposit in excess of $10,000 to a financial institution be reported through a CTR. Furthermore, any cash payment to any business in excess of $10,000 must be reported to the federal government on a Form 8300. By structuring deposit transactions to be below the federal reporting guidelines, cash can be placed into the financial system.

3. Carrying the money offshore to a country with bank secrecy and privacy laws can be used to place the money into the worldwide financial system.

Once in the financial system, a paper trail (actually, an electronic trail) of the money and its movement begins. Most money laundering schemes are most vulnerable to detection at or before the placement stage.

Layering: Layering is the second stage and is used to hide or disguise the source of the money. An inherent goal of layering is concealment of the true source and business to business, account to account, etc. in an attempt to disguise the money source and confuse investigators because the amounts are no longer equal to those originally received. Furthermore, the transactions may have seemingly legitimate
business reasons and may even have paper documentation that lends seeming legitimacy to the nature of the transaction. Layering may involve foreign countries, especially those countries where bank secrecy and privacy laws make it difficult, if not impossible, for investigators to continue to follow the money trail. Once in a foreign locale with a strong commitment to bank secrecy, the money can be moved to another bank account, possibly in another country that also with strong bank secrecy laws, with complete anonymity. By this time, the funds are ready for the last stage of money laundering (integration). By using currency and offshore bank accounts, a perpetrator can make it almost impossible to follow any sort of money trail.

**Integration**: Integration, the third and final stage, is the attempt to convert the placed and layered money back into the hands of the perpetrator in a form that the perpetrator can use without risk of prosecution for being associated with dirty money. As examples, integration can take the form of payment for consulting services to a business or individual to which the perpetrator appears to have no association. Integration may take the form of a loan for which the repayment terms may range from legitimate to non-existent. Recall that even if the perpetrator repays the loan, he or she is only repaying the proceeds to their own business or bank account. The main issue with integration is ensuring that the source of the money and the transaction itself appears to be legitimate.

The good news for investigators is that perpetrators have two choices: spend money that they cannot show came from legitimate sources or launder the ill-gotten proceeds so that it appears that the sources of their money are legitimate. If necessary, some perpetrators may even pay taxes on laundered funds to further the appearance of legitimacy and make it appear that the perpetrator is a normal, tax-paying citizen. One nice attribute of money laundering is that ultimately the money must start and end at the same spot. Thus, if the investigator identifies the ultimate beneficiary, he or she knows that the same person is controlling the activity on the front end. Likewise, if the investigator identifies the source of the laundered funds, he or she knows who ultimately must benefit from the money laundering activity.

While the Bank Secrecy Act of 1970 improved the financial reporting and record keeping associated with cash transactions, the Money Laundering Control Act (MLCA) of 1986 was the first time that money laundering itself was considered a prosecutable offense. The MLCA has been amended over the years to strengthen the laws and eliminate various loopholes as follows:

- 1988—Anti-Drug Abuse Act
- 1992—Annunzio-Wylie Anti-Money Laundering Act
- 1994—Money Laundering Suppression Act
- 1996—Terrorism Prevention Act
- 1996—Health Insurance Portability and Accountability Act
- 2001—USA Patriot Act

In order to prove money laundering, the government must demonstrate (1) that a financial transaction was either attempted or conducted, (2) that the defendant knew that the proceeds derived from some unlawful act, (3) the property derived from a specified unlawful act, and (4) that the defendant attempted to accomplish one of the following objectives:

1. Promote a specified unlawful act (SUA).
2. Conceal the nature, source, location, ownership, or control the proceeds of a SUA.
3. Attempted to avoid federal reporting requirements (e.g., $10,000 for a CTR).
4. Attempted to evade taxes.

Furthermore, if the money laundering activity involves the international movement of money, the perpetrator can be charged with violation of international money laundering sections of the federal statutes. One of the principal goals behind money laundering laws and regulations is that of seizure. The principle is consistent with that described earlier: to deprive the criminal of the use of their ill-gotten gains. The legal basis of the forfeiture is that the claim is made not against the alleged criminal, but against the property itself. Forfeiture requires probable cause that connects the property to an illegal act. The civil litigation threshold is a direct association between the criminal act and the property subject to seizure. In the criminal realm, courts will allow substitute property to be seized. Civil forfeiture funds are used to supplement the budgets of law enforcement agencies and are usually shared among the law enforcement agencies that participate in the investigation (providing an incentive to participate in a meaningful way).
Under federal law, all property involved in money laundering, as well as violations of the Bank Secrecy Act involving currency reporting, are forfeitable. To seize the funds of a money launderer, the federal government must be able to prove the elements of the money laundering offense. If money from a specifically unlawful act (SUA) is commingled with funds generated from legitimate sources, all of the funds are subject to confiscation. If the laundered money is then converted into other assets (e.g., stocks, bonds, homes, cars, etc.), the other assets are subject to forfeiture. Furthermore, if the other assets are in the names of persons other than those involved in the money laundering or criminal activity, the assets would still be subject to forfeiture. Criminal, civil, and administrative seizures are facilitated with a seizure warrant. In some cases where the property or its value may be at risk, a temporary restraining order may be obtained to prevent the transfer of title to the property or encumbering the property in some other manner.

Internationally, foreign countries have not always been as willing or able to attack money laundering in the manner in which it has been in the United States. In a post-9/11 world, more countries have started to cooperate in identifying and investigating money laundering activities. Some of the international commitment to anti-money laundering is demonstrated through such entities as the International Criminal Police Organization (INTERPOL) headquartered in France, the United Nations' Narcotics and Vienna Conventions, the British Commonwealth, which includes countries beyond Great Britain, a number of whom have been known as bank secrecy and tax havens, and the Organization of American States (OAS). In addition, the Financial Action Task Force (FATF), formed in July 1989 by the G7 (Britain, Canada, France, Germany, Italy, Japan, and the U.S.), the European community, and eight other nations analyzes international money laundering and makes recommendations for changes in banking and criminal laws. In recent years, the FATF also has started to investigate terrorism financing. The FATF has identified three times when money laundering is ripe for detection:

- Domestic entry into the financial system (placement)
- Transfers of fund abroad for the purposes of integration (layering)
- Transfers back to the originating country for repatriation (integration)

The Egmont Group is an association of financial intelligence units from around the world that share financial intelligence. Overall, it is now easier to obtain information from the international financial community than ever before. In addition, the United States is often able to gain or coerce assistance in the retrieval of moneys located in foreign lands. The mechanism for information sharing and money retrieval is the MLAT system or Mutual Legal Assistance Treaty.

Racketeering Influence and Corrupt Organizations Act (RICO)

Criminal organizations need a process to clean up their money. They also need an “organization” and bank accounts for money to enter the financial system and from which to initiate the money laundering placement stage. While money laundering is about the process used to make dirty money appear legitimate, RICO addresses the ORGANIZATIONS involved. Thus, RICO, enacted in 1970, the same year as the Bank Secrecy Act, is closely aligned to money laundering laws and regulations. While the original goal was to allow investigators to go after businesses and other entities involved in organized crime, it has been used to prosecute a wide variety of organizations including those associated with corrupt public officials, drug dealers, gangs, labor unions, and others.

Portions of the RICO Act outlaw:

- Investing illegal funds in another business
- The acquisition of a business through illegal acts
- The conduct of business affairs with illegal acts

Essentially, it is illegal for any person who has received funds that derived directly or indirectly from a pattern of racketeering to invest or acquire any other business that is involved in interstate or foreign commerce. It is also unlawful for persons involved in a racketeering activity to acquire or maintain any interest or control of any entity where the entity is involved in interstate or foreign commerce using illegal means such as fraud, extortion, bribery, or money laundering. Finally, a person employed by or associated with an entity involved in interstate or foreign commerce may not be involved in the operations of an enterprise’s affairs in a pattern consistent with racketeering or the collection of unlawful debt.

RICO provides for criminal penalties up to $25,000 and twenty years in prison. Like the money laundering statutes, RICO also provides for the forfeiture of assets used in racketeering crimes and permits
treble damages in civil cases. Individuals, corporations, and loosely organized “entities” may be prosecuted civilly and criminally under the RICO statutes. Racketeering acts include:

- Violent crimes such as kidnapping, murder, arson, and robbery
- Other felonies such as unlawful gambling, bribery, extortion, the distribution of obscene material, and controlled substance trafficking
- Violations of money laundering laws
- Violations of the Bank Secrecy Act
- Mail and wire fraud
- Labor offenses
- Securities fraud

RICO and the money laundering statutes are somewhat circular in that money laundering laws and regulation identify RICO violations as a SUA and RICO specifically names money laundering as a RICO offense.

**Conspiracy**

As noted above, criminals in complex crimes, frauds, and financial activities require a process, money laundering, to clean up their funds and require entities as a means of accomplishing their operational goals, laundering money, and as an integration option. The organizations and the money laundering process also require individual participants. Whereas money laundering statutes go after the process and RICO goes after the organizations, conspiracy targets the individuals involved in the illegal activity. Thus, conspiracy deals with the PEOPLE.

A conspiracy involves three elements:

1. The coconspirators must have an agreement (actus reus) between them.
2. The coconspirators must act or demonstrate an inclination to commit a crime.
3. The participants must mentally commit to the act through their state of mind (mens rea or intent).

From a practical perspective, prosecutors need to prove:

1. The existence of a conspiracy.
2. Willing participation in the conspiracy.
3. The defendant’s knowledge of the conspiracy.
4. At least one overt act was completed in carrying out the conspiracy.

Independent acts toward common criminal purpose may be linked together as a single conspiracy. Related to money laundering, conspiracy may be involved assuming that the coconspirator knew that the funds were coming from at least one specified unlawful activity. Conspiracy is also a specifically prohibited conduct under RICO.

The acts and statements of one coconspirator may be admissible against others involved in the conspiracy. Thus, lawyers and prosecutors will use conspiracy as a means of linking persons together and obtaining convictions of each of the coconspirators related to the underlying offense. The overt act required to prosecute conspiracy need not be illegal itself and may seem innocuous, such as sending an email or making a phone call, as long as the act is integral to the conspiratorial activity. While conspiracy charges have far-reaching implications, an entity and its employee cannot be coconspirators because they are legally viewed as one. However, an entity may conspire with another entity or with independent, third-party individuals.

**USA Patriot Act**

The USA Patriot Act is formally known as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act. Terrorism, like many crimes, is rooted in money. Money provides control, operating funds, and the means to acquire and maintain infrastructure. It is not coincidental that the 9/11 attacks chose to target Washington, D.C., the political hub of the United States and also to target New York, the U.S. financial center. At least one of the goals for targeting New York was to disrupt the international financial markets and wreak havoc on the American and Western economies worldwide.
CHAPTER 4  COMPLEX FRAUDS AND FINANCIAL CRIMES

Title III of the USA Patriot Act is the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001. Overall, the Patriot Act identified new types of money laundering crimes and increased the penalties associated with them. Specifically, the Patriot Act outlaws money laundering as follows:

- Funds generated from foreign crimes of violence or political corruption
- Funds generated from cybercrime
- Funds generated from offenses related to supporting terrorist organizations
- Funds related to bulk cash smuggling

In addition, the Patriot Act sets out the procedure for the forfeiture of bulk cash that had been smuggled. The felony penalty for bulk cash smuggling is five years. The anti-money laundering provisions of the Patriot Act supplement those discussed above. The Act also eliminated a prior requirement that the defendant knew that the proceeds being laundered had been generated from illegal business operations. Furthermore, the attempted transport of more than $10,000 in currency or monetary instruments into or out of the country is illegal if the funds are concealed and the transporter was attempting to avoid the U.S. federal reporting requirements.

The Patriot Act is particularly aggressive on the forfeiture of assets related to terrorism. The Act permits the confiscation of all property of an individual or entity who participates in the planning of a terrorist attack. Furthermore, any proceeds used to facilitate an act of terrorism or derived from a terrorist act are subject to forfeiture. If an individual or entity has assets in a foreign country and U.S. officials are unable to obtain those funds, the Patriot Act allows the seizure of funds from any correspondent banks where the terror organization has correspondent bank accounts. These provisions provide a significant incentive for financial institutions to avoid transactions associated with terrorists.

One of the techniques of terrorists and others interested in money laundering is to utilize shell banks, or banks that have no physical presence in any jurisdiction. The USA Patriot Act prohibits U.S. financial institutions from allowing correspondent account transactions with shell banks. The USA Patriot Act also increased the availability of banking records to investigators, increased due diligence requirements for banks, and established standards for customer identity verification. U.S. financial institutions are also required to have anti-money laundering programs in place. The U.S. Department of Justice has reported a number of successes as a result of the money laundering regulations that were improved by the USA Patriot Act, and these successes go beyond terrorism and terrorism financing to include the capture of fugitives, the prosecution of child pornography, the dismantling of complex cybercrime schemes, and the prosecution of drug and illegal weapons traffickers.

The Bank Secrecy Act

Like RICO, the Bank Secrecy Act (BSA) was passed in 1970 to assist in the investigation of illegal acts associated with drug trafficking and tax evasion. The BSA requires that financial institutions maintain adequate records and that financial institutions report certain types of transactions to the federal government. Any currency transaction in excess of $10,000 must be reported to the Department of the Treasury on IRS Form 4789, or the Currency Transaction Report (CTR). In addition, financial institutions may also report other transactions when the nature of the financial transactions or the activities of the persons involved appears to be suspicious. Such transactions or activities are reported on the Suspicious Activity Report (SAR). Because the CTR reporting requirements are more specific, the number of submissions tends to far exceed those of the SAR. In addition to financial institutions, businesses whose customers initiate transactions with more than $10,000 in currency or coin are required to file an IRS Form 8300. This form was originally designed to identify potential tax evaders and thus, the information was maintained within and only utilized by the IRS. Subsequent to 9/11, however, the information disclosed on Form 8300 has been made more widely available to law enforcement. The data from these submissions is collected and disseminated by the Financial Crimes Enforcement Network, otherwise known as FinCen.

Beyond the CTRs, SARs, and Form 8300s, the BSA has the following additional reporting requirements:

- The movement of more than $10,000 into or out of the United States must be filed on FinCen Form 105, Report of International Transportation of Currency or Monetary Instruments. Monetary instruments include negotiable checks, travelers’ checks, and bearer money equivalents.
THE U.S. BANKING SYSTEM

• The CTRC must be filed by casinos (the “C” tacked on to the end of CTR) when a person conducts a transaction in more than $10,000 in currency. Casinos are known for their elaborate and sophisticated surveillance methods and have the ability to track suspicious transactions

• The FBAR requires that each U.S. person who has a foreign bank account report its existence on Treasury Form 90-22.1, or Foreign Bank Account Report

• Any person who owns or controls a money transmitting business must register that business within 180 days of its creation. These businesses are required to maintain records and obtain customer identification for transactions in excess of $3,000, including the person’s name, address, passport number or taxpayer identification number, transaction date, amount, currency names, country, and total amount of each type of currency

The BSA attacks the placement stage of the money laundering process. It is at this stage where the money launderer is most vulnerable because they have control over funds from unexplained sources. Once the money launderer starts layering and integrating the proceeds, money laundering is difficult to identify because the true source of the funds has been concealed.

Mail Fraud

Mail fraud statutes may be invoked any time that a scheme to defraud someone has been devised by false or fraudulent pretenses, representations, or promises and such fraud takes place in any U.S. Post Office, U.S. mail depository, or through transport by the U.S. Postal Service. The person needs only to cause the mail service to be used to facilitate the fraud act, and the item sent or delivered may be transported by private or commercial carrier in furtherance of the fraud act. The violation is punishable by not more than a fine of $1,000,000 and imprisonment of up to thirty years. Thus, any time that the mail is used to facilitate a fraud, no matter how large or small a part the mail aspect may be, mail fraud may have been committed. Mail fraud is one of the workhorses of federal white-collar prosecutions and is available among other offenses to investigate and prosecute complex frauds and financial crimes. As an example, a person who mails a fraudulent tax return to the Internal Revenue Service has not only committed tax fraud but also committed a mail fraud offense. The mailing itself does not need to contain any fraudulent representation but must be integral to the overall fraud scheme. The scheme does not need to succeed or the intended victim suffer any loss for the mail fraud statute to be applicable.

Wire Fraud

While mail fraud occurs when a fraudster or other criminal utilizes the various mail services to facilitate a fraud, the use of wire, radio, or television to communicate false or fraudulent pretenses, representations, or promises is a violation called wire fraud. Unlike mail fraud, the electronic transmission must be associated with interstate or foreign commerce for wire fraud statutes to apply. The electronic communications may be writings, signs, signals, pictures, or sounds used to further the fraud scheme. Like mail fraud, a wire fraud violation is punishable by not more than a fine of $1,000,000 and up to thirty years of imprisonment.

THE U.S. BANKING SYSTEM

The banking system in the United States provides a number of services including mortgages, secured property loans (e.g., cars, recreational vehicles, trucks, boats, etc.), secured cash loans, credit cards, personal lines of credit, business loans, business lines of credit, letters of credit for overseas transactions, student loans, overdraft protection options, home equity loans, demand deposit accounts, time deposits, check writing and cashing services, periodic account statements, cashier’s checks, certified checks, money orders, bank drafts, travelers’ checks, and exchanges documents. Banks also facilitate currency exchanges, have trust department services, and provide personal banking services for high net worth individuals.

The benefit of the U.S. banking system is that everything is written down and most transactions and their backup documentation are captured on microfiche or some form of electronic imaging. Loan applications are the initiating point for bank loans. The bank then evaluates the applicant’s ability to repay the loan (debt capacity), the person’s willingness to repay the loan (character), the collateral offered by the borrower (if any), and other conditions such as the borrower’s employment history, prior loan experience with the type of loan sought, the overall economy, and any other conditions that might be applicable. As part of evaluating capacity to repay, the lending institution will obtain a credit report on the prospective borrower, prior tax returns, borrower W-2s and pay stubs, borrower investment statements, and other
CHAPTER 4  COMPLEX FRAUDS AND FINANCIAL CRIMES

borrower financial records. As such, the loan application file has a wealth of financial information included. Once the loan is approved, the loan documents are signed, and funds are transferred, the financial institution maintains meticulous records concerning repayment. If an investigator is able to obtain a subpoena for the loan records, these should be reviewed carefully not only for the financial information but also for leads to other individuals, accounts, businesses, etc.

Banking records for regular checking accounts owned by individuals and entities also contain a wealth of information. The signature card contains the names, Social Security numbers, and signatures of all persons able to withdraw funds from the account. The initial deposit may be an employment check or a check drawn on another account. In either case, this information can be quite valuable. Once the account is opened, the detailed activity can be analyzed from the monthly statement and supporting documentation that accompanies that statement to develop patterns of spending habits, a profile on the account holder, the financial condition of the account holder, changes in activity patterns, and the timing of those changes. All of this information can be useful during an investigation. The depository activity should also be analyzed. Deposits may come from employers, in the form of cash, from investment accounts, friends, businesses, business associates, ATM deposits, wire transfers, mail, and other sources within the bank. While each of these may hold important clues and linkages to businesses, people, and places, wire transfers, particularly those into and out of the country, should warrant special attention. The check itself may contain valuable information.

In the example in Figure 4-1, the 0905 is the check number that also appears on the bottom line. The 48–567 over the 1234 is a code that identifies the issuing bank. The numbers above the line, 48–567 are the ABA (American Bankers Association) transit number: the first number, 48, represents the state where the bank is located and the second, 567, is a code that ties to the issuing bank’s name. The number below the line with the numbers 1234 is the Federal Reserve Routing Code: the first two digits represent the Federal Reserve District, the third number identifies the District Office, and last digit indicates when the cash proceeds should be made available, assuming that the issuing account has sufficient funds. The payee is Innovative Learning Place. The amount or face value of the instrument is $53.21. The paying bank is First Huntington Commerce Bank. The following string of numbers are magnetic ink character recognition or MICR numbers:

12345678910 002398765410 905 2125 : 0000053.21

12345678910 is a combination check routing number (1234) and, ABA transit number (567 plus 8910). The numbers 002398765410 represent the checking account number of Jimmy–Jo Venture Capital. The number 905 is the check number in MICR format. The number 2125 is the process code and the number 0000053.21 represents the check amount or face value.

Check 21, Check Clearing for the 21st Century Act, went into effect on October 28, 2004. This Act effectively allows the first bank to touch a check to image the front and bank of the check and then shred the original. Investigators will have access to the electronic images that can serve as evidence. The check is then processed almost instantly. With the advent of efficient and effective EFT (electronic funds transfer), electronic payment via the Internet, and debit cards, the paper check will become scarce over time. Although the backs of checks will change, the front of paper checks will contain the same information under Check 21 as they have in the past. The items reviewed above may provide valuable clues such as connections between individuals, businesses, and physical locations as well as other clues. This information should be carefully evaluated to further the investigation.

Cashiers’ checks, money orders, and travelers’ checks are favorites of money launderers. Once purchased, these monetary instruments facilitate the easy movement of large sums of money. Cashiers’ checks,
money orders, and travelers' checks are very transportable and are accepted by most financial institutions. The primary drawback is that the initial transaction has a significant amount of documentation with it.

Cashiers' checks are often used as a down payment for big-ticket items such as homes, cars, boats, etc. Despite the amount of documentation available, because the check is tied to a bank's checking account instead of that of an individual, the tracing of these instruments can be complicated. Cashiers' checks come with three copies, the original check (top copy), a copy for the bank's records, and a copy for the customer. In addition, the bank teller logs the check in a ledger. If the acquisition involves cash greater than $3,000, that fact will be noted in the log. Cash in excess of $10,000 generates a CTR. If the proceeds are generated from the customer's bank account, tracing the check becomes a little easier. If the goal of the investigator is to identify all checks with the customer's name associated with it, the bank will usually require the branch name and the approximate date as a starting point. Because the only record is the log or ledger, tracing cashiers' checks can be difficult.

Money orders typically have limited dollar amounts. For example, at the U.S. Post Office the largest money order is $700. Travelers' checks can be traced only by serial number, so the investigator needs a starting point there as well. Otherwise, tracing travelers' checks can be very difficult. Bank customers may also rent a safe deposit box. Banks have no means of knowing the contents of these boxes, and access is strictly limited. An investigator cannot gain access without the use of a search warrant. The safe deposit box records include a rental application, and the bank keeps detailed record of access to the box including the date, time in, time out, and the person signing in.

Investigators may run across a number of different types of banks. Commercial banks are those most persons are familiar with. Other persons have accounts at federal savings banks (also known as savings and loan banks). Savings and loans got into significant financial trouble in the 1970s and 80s by speculating in commercial real estate. Since that time, regulation of these banks has been changed to avoid a similar crisis.

Offshore banks exist in foreign countries. It is not uncommon for high net worth U.S. citizens to bank internationally to take advantage of the various banking and tax laws. Criminal types, however, often attempt to exploit the secrecy laws of other countries' banking systems to hide their own nefarious activities, including money laundering. An investment bank underwrites the securities of companies issuing stocks and bonds to investors. The investment banker buys the securities and then resells them to the investing public at a preordained date.

Private banks are established by individuals and businesses to facilitate transactions. Many U.S. banks offer private banking to high net worth individuals. Private banking arrangements often come with various privileges and services not provided to regular clientele.

Central banks, such as the U.S. Federal Reserve, are responsible for maintaining and protecting the country's currency. Correspondent banks provide banking services for another bank's customers where the other bank does not have a local branch operation or other physical presence. Cyber banks are available on the Internet. Other banking arrangements include credit unions, auto finance companies, bank holding companies, and securities brokerages.

Businesses competing internationally will usually require international banking services as well as those located domestically. Typically, international banking customers do so for privacy reasons, to enhance security (especially true for unstable countries and their local banking options), convenience, and financial benefits such as tax breaks, better interest rates, longer float, etc.

**MOVING MONEY INTERNATIONALLY**

In order to transact business internationally, most companies also need to issue forms of payment that complement normal check disbursements through the domestic checking account. Some businesses located in foreign locales require cash payments in advance. This cash flow timing is advantageous for the provider of goods and services but has the potential to put the buyer in a cash flow crunch. As a substitute for cash in advance, some providers of goods and services accept documentary letters of credit. This is a common form of international payment because both the buyer and seller are afforded some protection.

The bank operates as the honest third-party broker. The bank essentially guarantees the provider of goods and services payment, assuming contractual performance as soon as the buyer confirms that the terms and conditions have been met. In advance of the transaction, the buyer specifies the documentation required in order for the seller to be paid. Such details may be the subject of negotiation between seller and buyer. Once the goods and services have been provided, the seller provides the required documentation to
the bank, including the sign-off of third-party shippers and other agents to the transaction. Upon receipt of the documentation, funds are transferred from the buyer to the seller as agreed upon in the contract. The documentation typically includes a bill of lading issued by the transporter, a certificate of inspection by an agent of the buyer, certificate of manufacture by the seller, certificate of origin, commercial invoice, the draft bill of exchange, a copy of the export license of the seller, the buyer’s import license, and any insurance documents required as part of the transaction.

Documentary collection, a third form of international payment, is similar to domestic cash on demand (C.O.D.). Essentially, title for goods purchased is held until payment is made. Upon payment to the seller, the intermediary bank provides the documentation to the buyer. Because this is a documents-only transaction, the buyer has little protection against poor quality. Open account is the fourth international payment method and is virtually the opposite of cash in advance; under this arrangement, the seller is at risk until the buyer pays.

Trillions of dollars move around the world every day. The knowledge of how much money flows also indicates the difficulty that persons engaged in anti-money laundering activities face. Most of the trillions of dollars in money movement are legitimate. The number of transactions and relative dollars that are associated with money laundering are relatively few in number and small in amount (estimated to be 1 percent or less of all international movements). This money moves around the world electronically, in the form of electronic funds transfer (EFT). Cyber banking, smart cards, prepaid phone, debit, credit, and gifts cards and other similar methods for the movement of money will only ensure that the amount of money moving around the world increases as time goes by. As examples, electronic money flows are engaged by banks, businesses, credit card companies, money transmitters, governments, investment brokerage, stock exchanges, and commodity dealers.

Any electronic transmitter of money located in the United States must register with FinCen as a money services business (MSB). Money transmitters can be large, such as American Express, CitiBank, Bank of America, or can be relatively small businesses. Transmitters use a messaging system. The message communicates that money has been received on one end of a transaction and is available at some other place around the world for pickup. Typically, the person picking up the money must identify himself by name or some other security measure. The transmitters who facilitate the transaction for their customers collect a fee for their service. Federal law requires identification by the customer if the transfer involves cash in excess of $3,000. A CTR is required for cash transfers in excess of $10,000. Because of the ease and speed of movement and relative anonymity, electronic funds transfer around the world is a favorite tool for use by money launderers.

In addition to relatively small money transmitters, three systems exist for major money movement. First, Fedwire is the primary mechanism for domestic wire transfers in the United States and connects all of the twelve Federal Reserve Banks in the United States and approximately 12,000 domestic financial institutions. Fedwire may process 300,000 transactions a day, encompassing hundreds of billions of dollars. The second system involved in electronic funds transfer is the Clearing House Interbank Payments System (CHIPS). CHIPS serves as the main EFT system for processing international electronic transfers of money. CHIPS handles almost a trillion dollars a day in transfers among over 130 banks in more than thirty countries. CHIPS fund transfers are supported by the Society for Worldwide Interbank Financial Telecommunications (SWIFT). SWIFT is the messaging system that handles the communications by banks that accompany most CHIPS transactions. SWIFT is analogous to an email system. The messages over SWIFT initiate most of the transfers made with the CHIPS system. Telex provides a similar system to SWIFT to which businesses can subscribe.

Numerous records are generated with an electronic funds transfer. First, the person requesting the transfer must complete a transfer request. At the completion of the transactions, a confirmation is generated. In addition, debit and credit memos and various other documents, logs, and ledger transactions are created during the transaction.

In addition to the formal bank systems, domestic and international, informal arrangements exist as well. Hawala is an informal banking system originally created to support immigrants located around the world. Hawala (meaning “trust”) allows transfers of money between individuals with no record of the transaction. This money transmission system is international, informal, and unregulated. A person that wants to move money goes to his local contact and gives the money to the person, as well as instructions concerning who will collect the funds at the destination. The local Hawala representative then makes a call to his contact at the destination and communicates the instructions for collection. The Hawala representative at the destination then provides the funds to the recipient. Of course, the Hawala representatives collect fees for their services. The Hawala system is based on trust and is fast, efficient, unregulated, and maintains
almost no paperwork so the transactions are made in a relative vacuum. The value of such a system to money launderers cannot be overemphasized.

To investigate money movement through wire transfer, the investigator generally needs a lead and a customer bank account. Thus, the focus is on the beginning point of the wire transfer. From there, the investigator can obtain a subpoena and visit local branches to determine whether such movement has taken place. The data gathered, if found, should include the name and address of the originator, the amount, date, remittance instructions, the beneficiary, the recipient bank, and any other pertinent information captured during the transaction.

OTHER COMPLEX FRAUDS AND FINANCIAL CRIMES

Tax Evasion and Fraud

The Internal Revenue Service (IRS) is responsible for determining, assessing, and collecting taxes imposed by Congress. The IRS is divided into four major divisions:

• Wages and Investment
  • Small Business/Self-Employed, including Excise Taxes
  • Large and Mid-size Business Division (in excess of $10 million in assets)
  • Tax-exempt and Governmental Entities

The IRS also has smaller divisions that deal with appeals, communications, and liaisons and criminal investigations. The Criminal Investigations Division (CID) is the law enforcement arm of the IRS. The IRS has responsibility for a number of taxes imposed by Congress including personal income taxes, corporate income taxes, employment taxes, including FICA (Social Security), Medicare, and federal unemployment tax (FUTA), excise taxes, and estate and gift taxes. In addition to federal income taxes, states, counties, cities, and other municipalities also assess and collect taxes including personal income taxes, corporate income taxes, state unemployment taxes, personal property taxes, sales and use taxes, and other taxes as required by those jurisdictions.

The primary distinction in whether an individual or entity has committed tax fraud or simply committed an error is the intent of the individual. The intent of the party to the tax return will determine the difference between tax errors and tax evasion. Tax avoidance consists of using legal means and methodology to minimize taxes within the existing framework of tax rules and regulations. Tax evasion is the intentional wrongdoing to evade taxes believed to be owed. Tax evasion is fraud and implies bad faith, intentional wrongdoing, and a sinister motive.3 One defense against tax fraud is an objectively reasonable "good faith" misunderstanding of the law. The belief that taxes are unconstitutional is not considered objectively reasonable. Thus, tax evasion (fraud) requires an intentional wrongful doing with the specific purpose of evading a tax known or believed to be owed. Furthermore, tax fraud requires that the defendant have taxes owing, and evasion requires at least one "affirmative act" to demonstrate intent. Affirmative Acts are compelling and are actions that establish intent (deliberate action), often focusing on concealment. Common tax evasion schemes include:

• Deliberate understatement of taxes owed
• The omission of taxable transactions and activities
• Fictitious events and activities
• Hidden events and activities
• False statements made to tax agents
• False documentation to support fraudulent tax filings

Examples of affirmative acts include the following:4

• Deceit—Lying when giving statements
• Subterfuge—An artifice to hide an act (evade a rule)
• Camouflage—to hide
• Concealment—to hide
• Coloring events to making them appear different
• Obscuring events to making them appear different
In contrast to affirmative acts, affirmative indicators are not deemed compelling in and of themselves, but are considered badges of fraud, red flags, symptoms, or signs of potential fraudulent conduct. Badges of fraud arise in a number of areas:

- **Actions of the Taxpayer:**
  - Previous tax filings but the taxpayer stops without reasonable cause
  - The taxpayer correctly classifies transactions for some suppliers/vendors but not for others (e.g., unusual source)
  - Taxes have been passed on to customer but not reported or paid
  - The taxpayer handles identical products but considers one to be taxable and the other nontaxable

- **The Treatment of Income:**
  - Omissions of specific revenue sources
  - Omission of revenues from specific products
  - Omission of revenues from product lines
  - Omissions of entire sources of revenue
  - Unexplained failure to report revenue

- **The Treatment of the Books and Records:**
  - Two sets of books and records
  - False entries or alterations
  - Backdated or postdated documents and transactions
  - False invoices
  - False applications
  - False financial statements
  - Invoice numbers that do not make sense
  - Failure to keep and maintain records
  - Concealment of records
  - Refusal to make records available
  - Unexplained variances between returns and the underlying books and records

- **Related Parties**

- **Conduct of Taxpayer:**
  - False statements
  - Interference with tax agent’s examination
  - Failure to follow the advice of attorneys/accountants
  - Less than full disclosure
  - Taxpayer knowledge (e.g., taxpayer has an accounting degree)
  - Testimony of employees or other unrelated third-party individuals
  - Destruction of books and records
  - Transfer of assets to conceal their true nature or their ownership
  - Patterns inconsistent over time
  - Attempts to bribe the examiner

The process of investigating tax fraud starts with first indications (badges of fraud) and concludes with either a finding of no fraud or a finding of tax evasion due to the presence of affirmative act(s). Consistent with other fraud examinations, when attempting to prove intent, investigators may find it helpful to consider the following:

- Present evidence in chronological order, particularly examining the timing of key transactions
- Identify altered, concealed, or destroyed documents or evidence (e.g., deliberate backdating)
- Carefully record false statements by the taxpayers
• Look for pattern or repetition of suspicious behavior
• Obtain the testimony of coconspirator
• Obtain a confession from the taxpayer

If predication exists that tax fraud may be present, the following is a seven-step process to convincingly resolve any badges of fraud.10

Step 1—Consider the risk of fraud by brainstorming, considering how and where tax return information might be susceptible to fraud, how and where tax return fraud might be hidden, and exercising professional skepticism.

Step 2—Obtain information needed to identify the risk of fraud by interviewing owners, management, internal auditors, and clerks, and carefully documenting their statements, considering the results of analytical and preliminary examination procedures and any other observed badges of fraud.

Step 3—Consider policies, procedures, and controls in place to prevent fraud by understanding the internal control environment; evaluating whether policies, programs, and controls are operational; evaluating whether policies, programs, and controls address the identified risks of fraud; and drawing conclusions about the risk of fraud.

Step 4—Respond to the results of the risk assessment steps. Specifically, as the risk of fraud increases, the agent or criminal investigator should respond with more creative procedures and investigative techniques, utilize more nonfinancial performance metrics, consider the need to gather additional evidence, and consider altering the nature and extent of examination procedures.

Step 5—Evaluate the evidence by continually assessing the risk of fraud throughout the examination, evaluating results of analytical and examination procedures performed, and reevaluate the risk of fraud near completion of fieldwork.

Step 6—Draw conclusions by obtaining taxpayer explanations for errors, misstatements, omissions, and other irregularities, corroborating explanations, and making any necessary judgments. Step 6 may need to be completed in concert with the investigator’s manager or one of the IRS’s Fraud Technical Advisors.

Step 7—Communicate about the tax evasion (fraud) by making sure that all aspects of the investigation have been properly documented, and write the required reports. After consultation with a Fraud Technical Advisor, the investigator prepares an IRS Form 2797 (Referral Report of Potential Criminal Fraud Cases) that includes a detailed factual presentation including:

• Affirmative acts
• Taxpayer’s explanation
• Estimated criminal tax liability
• Method of proof used to determine taxes owed

When an examiner discovers failure to file, he or she must document the affected taxable periods, the explanations of the taxpayer, and determine if badges of fraud exist. Investigators should be careful about accepting the taxpayer’s assertions or explanations without grounding the statements in the evidence.

Like other frauds, the burden of proof falls on the investigating agent. Tax-evading persons can be pursued civilly or criminally. The primary determinant is what the investigating agent and their supervisors and managers believe that they can prove. Civil cases never rise to the level of overtly deliberate acts to evade taxes, and criminal cases involve behavior deemed too deliberate to be dealt with civilly. For example, the failure to cooperate or the maintenance of two sets of books and records might be considered so egregious that criminal pursuit is the only proper disposition.

Taxpayers have several defenses that should be evaluated as the investigator winds up his or her investigation. First, the taxpayer may argue that no taxes are due. Second, the taxpayer may claim that their scheme was set up to avoid rather than evade taxes owed. Third, the taxpayer may claim that the unpaid taxes were based on an objectively reasonable position based on a reasonable evaluation of the tax law, regulations, and prior court findings. Fourth, related to taxable revenues, the taxpayer may claim that they did not have unrestricted access or rights to the funds. Other defenses that may be presented and need to be evaluated include the mental competence and capacity of the taxpayer, the competence of paid bookkeeping services, ignorance of a complicated tax law, the innocent spouse defense, and reliance on an accountant or attorney. The innocent spouse defense is particularly applicable now that returns can be filed electronically without the signature of all parties to the return.
CHAPTER 4 COMPLEX FRAUDS AND FINANCIAL CRIMES

Bankruptcy Fraud

All bankruptcy cases are filed in federal court at the local district of the U.S. Bankruptcy Court. The Office of the Trustee, within the Department of Justice, is responsible for administering bankruptcy cases including appointing trustees, examiners, Chapter 11 committees, overseeing and monitoring trustees, reviewing employment and fee applications, and appearing in court on matters of interest to the estate and creditors. Within the Office of the Trustee, special investigative units investigate criminal referrals and complaints in bankruptcy cases. These units sometimes work with the Internal Revenue Service and FBI when the circumstances warrant cooperation as well as when jurisdictional issues arise.

Examiners are sometimes appointed in reorganization (Chapter 11) bankruptcy cases, particularly when assertions of fraud and misconduct by the debtor in possession have been alleged. In reorganization, the debtor in possession’s primary goal is to preserve and protect the assets and operations while the plan of reorganization is developed and subsequently confirmed by the bankruptcy judge. Secured and unsecured creditors hold claims against the bankrupt entity. Secured creditors hold some claim of collateral, which acts to protect the value of their claim against the bankrupt entity. Because security claims are typically filed at the state level (e.g., UCC (uniform commercial code) filing), the bankruptcy court must examine and rely on state law to determine the validity of secured claims against collateral. At the time of the bankruptcy filing, an automatic stay precludes any creditor, secured or otherwise, from taking any action detrimental to the health and well-being of the bankrupt entity. When the bankrupt estate is settled, secured creditors’ claims have priority over those of the unsecured creditors.

The bankruptcy code of the United States has several chapters:

- Chapter 1 contains general provisions
- Chapter 3 provides guidelines for bankruptcy case administration
- Chapter 5 establishes the rights and obligations of the creditors, debtors, and the estate
- Chapter 7 deals with the liquidation of the debtor’s assets, including individuals and businesses
- Chapter 9 applies to municipalities
- Chapter 11 contains provisions for those debtors hoping to reorganize and emerge from bankruptcy
- Chapter 12 is designed to address the needs of farmers and fishermen
- Chapter 13 contains reorganization bankruptcy provisions for high net worth individuals who cannot qualify for Chapter 7 liquidation

The bankruptcy court has the right to appoint a trustee in cases where there are claims of fraud, dishonesty, incompetence, or gross mismanagement if such appointment is in the best interest of the creditors, equity holders, and others with an interest in the estate. When a trustee is appointed, allegations of fraud and gross misconduct often underlie the appointment. In Chapter 7 cases, the trustee must investigate the affairs of the debtor. In Chapter 11, the duties and responsibilities are more far-reaching and include taking control of the business and making operational decisions.

One of the roles of the trustee is to attempt to identify missing assets and locate them, if possible. To do so, the trustee normally has access to the bankrupt entity’s attorneys as well as the accountants and their work papers, tax returns, and client books and records. To fulfill their fiduciary responsibilities, the trustee may need to gather information, not only from the bankrupt entity’s books and records, but also from banks, customers, related parties, suppliers, employees, pension funds, and others as needed. Once gathered, the trustee may consider the following investigative procedures:

- Reconstruct cash receipts and disbursements journals and general ledgers
- Identify new bank accounts, related party transactions, and hidden or concealed assets
- Take depositions of uncooperative witnesses
- Take depositions of third-party witnesses and others who can authenticate and corroborate documents, records, transactions, and other information
- Take declaration testimony from cooperative witnesses
- Interview witnesses
- Prepare an investigative report
- Submit a copy of the report to the U.S. Attorney’s Office if allegations of fraud appear justified
Bankruptcy crimes are investigated by the FBI and prosecuted by the U.S. Attorney’s Office, if warranted. The penalty for each bankruptcy offense is a fine of up to $500,000 and imprisonment for up to 5 years, or both. Title 18 of the U.S. code identifies nine offenses:

Paragraph 1—Knowingly and fraudulently concealing property from a custodian, trustee, marshal, or other officer of the court. Property is defined not only as assets, but also as books, records, and anything of value.

Paragraph 2—Knowingly and fraudulently giving false oath or account, including oral testimony during depositions, hearings, and trials.

Paragraph 3—Knowingly and fraudulently giving false declarations, certifications, verifications, or statements, including written documents such as the debtor’s petition, bankruptcy schedules, statement of affairs, interim statements, operating reports, and declarations in court such as court filings and motions.

Paragraph 4—Knowingly and fraudulently giving false proof of claims against the bankruptcy estate by creditors, agents, attorneys, or others on behalf of a claimant.

Paragraph 5—Knowingly and fraudulently receiving any material amount of property from the bankruptcy estate, including creditors or any other person.

Paragraph 6—Knowingly and fraudulently giving, offering, receiving, or attempting to obtain money, property, remuneration, compensation, reward, advantage, or promises for acting or agreeing not to act, including the bribery or attempted bribery of a court official.

Paragraph 7—Knowingly and fraudulently transferring or concealing any property in contemplation of a bankruptcy filing (i.e., pre-bankruptcy actions).

Paragraph 8—Knowingly and fraudulently destroying and altering documents during or in contemplation of a bankruptcy filing, including concealing, mutilating, falsifying, or making false entries in the books, records, documents, or papers relating to the bankrupt estate’s property or financial affairs.

Paragraph 9—Knowingly and fraudulently withholding books, records, documents, or papers relating to the bankrupt estate’s property or financial affairs from a custodian, trustee, marshal, or other officer of the court.

Title 18 also outlaws embezzlement against the estate. Bankruptcy fraud includes schemes to file a false bankruptcy petition, file documents during a proceeding, or make false or fraudulent statements, representations, claims, or promises before or after the filing of a bankruptcy petition. This applies not only to the actions of debtors and claimants during a legitimate bankruptcy, but also to the efforts of perpetrators to use bankruptcy as part of a scheme to defraud others, such as a bust-out scheme. Common bankruptcy schemes include concealing assets (most common), the planned bust-out, multiple voluntary bankruptcy filings, the credit card bust-out, forged filings, and filings by petition mills on behalf of unsuspecting clients. The planned bust-out includes the setting up of a seemingly legitimate business, buying goods on credit, selling those goods, closing the business, and disappearing while leaving the creditors unpaid. The credit card version is similar except the fraud beneficiary is the individual cardholder instead of the business.

FROM THE FRAUDSTER’S PERSPECTIVE

Adapted from the whitecollarfraud.com blog by Sam E. Antar
Tuesday, October 16, 2007

A Warning to Wall Street Analysts from a Convicted Felon

To Wall Street Analysts:

During my years at Crazy Eddie, I found that securities analysts often did not know how to ask intelligent questions. When they asked intelligent questions, they did not know how to formulate the proper followup questions to our deceptive answers. Most Wall Street analysts were too trusting of the answers that they received from us.

Good questioning will often result in irritable behavior from company management. However, you are not doing your job to be in management’s good graces. Your job is to obtain not readily apparent facts, analyze them properly, and communicate them accurately and effectively to your readers. Top-notch financial journalist Herb Greenberg advises that you consider “what many companies don’t say as they spin the story their way.”

For example, be careful of corporate managements that

• accentuate positive information and spin and deflect negative information
• blame others for their company’s problems
• attempt to intimidate you

Beware of companies that exclude critics and provide “selective” access to management. Too often, Wall Street
It’s not about gaining access at the cost of your professional integrity. It’s about understanding what is really happening and communicating it accurately and effectively to your readers.

I played you analysts very well by rewarding you with selective access as the CFO of Crazy Eddie. I had you eating out of my hand with “selective” disclosures and “favored” access. While you craved for access and wrote your glowing reports in gratitude for your coveted access, you unwittingly helped make the frauds that we perpetrated at Crazy Eddie easier.

If you had any backbone, you would all boycott any presentation that excludes the more skeptical professionals among you. Frankly, after reading many transcripts lately, you guys look like amateurs with your lack of questioning skills, your inability to ask proper follow-through questions, and obtain straight, clear, unambiguous, and honest answers.

You seem like hand-picked patsies as I read your unchallenging questions and the lame answers that management gives you without any challenge or follow up. You never seem to learn as you compete with one another for the affection of management and let access to them rule your work at almost any cost.

Eventually you will run into a guy like I was. You will wish you asked the proper questions and follow-up questions too. You will wish that your other peers attended the meetings and asked questions you would not ask or could not ask. The questions that will never be asked by you and others will cause you to miss detecting the lies and deceit being spun upon you.

When the “earnings surprises” eventually come out, your previous work will be considered negligent and amateurish. Your future work will always be under a cloud of suspicion. You will be remembered for the glowing reports you made as management ran circles around you. Do you want people to think you are fools?

The managements that spread deceit and lies to the selective few who gain coveted access are not your friends. They are using your humanity against you as a weakness to be exploited in furtherance of their crimes. They know about how your efforts at coveted access end up corrupting your professionalism. They don’t care about what happens to you as a result of their actions. As a criminal, I never cared about you, too. You have been warned.

Respectfully,

Sam E. Antar (former Crazy Eddie CFO & convicted felon)

P.S. I see that nothing much has changed since my time. Keep it up. When a company that you wrote a glowing report on ends up a train wreck, will these same managements rescue you?

Securities Fraud

The Securities Act of 1933 is otherwise known as the “truth in securities act.” This Act deals primarily with the initial issuance of securities including stocks, bonds, treasury stock, debentures, investment contracts, puts, calls, straddles, options, some oil and gas investments, and other investment vehicles known as securities, focusing on full and fair disclosure. The Securities Exchange Act of 1934 focuses on the regulation of investment securities after their initial offering to the public. The 1934 Act contains a full range of anti-fraud measures. The 1933 and 1934 Acts were followed by the Investment Advisor Act of 1940, the Investment Company Act of 1940, and the Sarbanes–Oxley Act of 2002. The following outlines some of the more common securities fraud schemes.

Pyramid Schemes. In a pyramid scheme, fees or dues are paid by new members to join the organization. The new member, upon joining, is expected to attract and sign up new members and collect their membership fees on behalf of the organization. The organization generates cash flow, not by selling goods and services to clientele but by the collection of membership fees from new members. The membership fees are then distributed in part to the old members as a form of return on investment (e.g., dividend) to keep the old members attracting new members and to keep the scheme from collapsing. The scheme is dependent not only on the distribution of cash to old members, but also on the solicitation of new members and the collection of their membership fees as a source of funding distributions to old members. If the old members either fail to see returns on investment or fail to solicit and sign up new members, the scheme collapses, as they all invariably do.

“Prime Bank” Fraud. Though this fraud scheme, like most others, has various derivations, usually, investors are promised high rates of return with little inherent risk by investing in “prime bank” notes. The underlying methodology is supposed to be an offshore trading program that yields extremely high rates of return. The investment prospectus is usually confusing and makes reference to legitimate banks and recognized financial institutions from around the world. The prospective investor is usually required to sign a nondisclosure agreement. Of course, the entire investment is a sham and the investor will lose all of their money in the process.
Churning. Churning is the excessive sale of securities by a broker for the purposes of generating commissions. To prove churning, the alleged victim must prove that the broker controlled the trading in the account, the volume of activity was excessively high when compared to the investor’s trading objectives, and the broker acted with intent to defraud or with reckless disregard for the investor’s interests. According to the ACFE Fraud Examiners Manual, the best method for evaluating a claim of churning is to calculate the percentage of monthly commissions generated from the average account balance. Given this calculation by month, the investigator can look for signs of churning such as these:

- The percentage of commission increases during periods of less market volatility
- The percentage of commission increases over time but not in relation to the average account balance (which presumably stays the same)
- The gross commissions for some months are substantially higher than other months, and the underlying rationale for the trades is questionable
- The average gross commissions exceed 5 percent of the average monthly account balance
- The trades generated gross commissions but generated little or no realized investment gains
- The pattern of price changes in the securities sold, subsequent to the sale of the securities, is inconsistent with a need to sell the securities

And the investigator can ask these questions:

- Was the broker acting alone or as a result of investment recommendations and appropriate analysis?
- Did the broker make unauthorized trades?

Unsuitable Recommendations. Securities professionals are supposed to understand their customer’s investing objectives, their customer’s financial profile, and the customer’s level of sophistication. Placing customers in inappropriate investment vehicles is prohibited, and brokerages are supposed to have due diligence procedures in place to ensure that brokers are not abusing their trading responsibilities.

Parking. Parking is a technique used by an investor to avoid ownership reporting requirements and net capital rules. The parking investor sells the security to another individual with the intent and ability to repurchase the security at a later date with the intent of avoiding ownership reporting requirements and net capital rules.

Front Running. Front running is a derivation of insider trading. The perpetrator, possibly a back office clerk or exchange floor order filler, becomes aware of a large buy or sell order, a trade large enough to move the market. In advance of executing the large order, the perpetrator makes a trade in his or her account so as to benefit from the large order trade and the subsequent movement in the market.

Bucket Shops. Bucket shops act as a normal licensed brokerage business, but neither the enterprise nor its employees are registered or licensed. Such operations are illegal and usually created with the intent to defraud prospective clientele.

Misuse or Misappropriation of a Customer’s Securities. This scheme involves the theft of investment securities from a client’s account or the use of those securities as collateral for other transactions such as loans or margin trading. Periodically, such abuses are observed in trust accounts where few persons are monitoring the investments or the account activity.

Market Manipulations. Market manipulations usually occur in penny or micro-cap stocks, those with very small market capitalization. The manipulation occurs when trading activity is designed to artificially move the security price in one direction or another to give the appearance of activity and momentum to entice others to buy or sell.

Insider Trading. The use of nonpublic information by insiders with fiduciary responsibilities to their company and its shareholders in order to profit from the purchase and sale of securities is illegal.

**REVIEW QUESTIONS**

4-1 What is the difference between a predator and an “accidental fraudster”?

4-2 Why does collusion pose unique prevention and detection challenges?

4-3 How is the concept of an “organization” involved in mixing illegal activities with legitimate ones?

4-4 What is the difference between “following the money” and “tracing the money?”
CHAPTER 4 COMPLEX FRAUDS AND FINANCIAL CRIMES

4-5 Why is financial statement fraud often considered a complex fraud?
4-6 What are the different types of schemes associated with complex frauds?
4-7 How are the objectives of terrorists and organized criminals different?
4-8 What are the different types of banks in the U.S. banking system? How are they different?
4-9 What is the difference between tax avoidance and tax evasion?
4-10 How have some of the more common securities fraud schemes been perpetrated?

ENDNOTES

2. Ibid., 4
4. Internal Revenue Manual, 25.1.1.2.4
5. Internal Revenue Manual, 4.24.8.3
6. Internal Revenue Manual, 25.1.2.2
7. Internal Revenue Manual, 25.1.2.2
8. Internal Revenue Manual, 25.1.2.2
9. Internal Revenue Manual, 25.1.2.2
10. Modified and adapted from SAS No. 99
11. 2005 ACFE Fraud Examiners Manual, section 1.309