White Paper

Fraud and Money Laundering: Can you think like a bad guy?

February 2012 | Last updated July 2014

LexisNexis®

Risk Solutions

Table of Contents

Introduction 3

Five elements of fraud 3

Thinking like the bad guy 6

- Generic Fraud 6
- Specific Fraud 6

What the bad guy looks for (opportunity) 6

Fraud in motion 6

Case study 7

End game 7

About the author 8

Introduction

When it comes to fraud and money laundering, can you think like a bad guy? The truth is, we all can. However, many of us do not realize this fact. More importantly, most of us possess a high level of personal integrity that precludes us from considering the temptation of accepting the opportunity to commit fraud. Unfortunately, a good number of people do succumb to the lure of fraud. The frauds these unscrupulous individuals perpetrate can be extremely devastating. This was never more evident than it has been in recent years when we experienced the global financial crisis. To a great extent, fraud was the root of the problem that caused the economic distress we experienced.

Fraud takes many shapes. It can occur internally or externally. The criminal activity at the heart of the financial crisis was subprime loan frauds, mortgage fraud, corporate fraud and investment fraud (Ponzi schemes). Other significant financial frauds include insider trading, bankruptcy fraud, credit card fraud, embezzlement, check fraud, loan fraud, and identity theft and fraud. The success of these schemes, usually hinges on the ability to safely launder the proceeds of the illicit acts.

There is an important nexus between fraud and money laundering. Any discussion regarding fraud should include money laundering. To succeed, fraudsters must have a mechanism to legitimize their ill gotten gains. Laundering the proceeds of fraud provides an air of authenticity and more importantly, immediate access to the funds.

The poster child for the nexus between fraud and money laundering is Martin Frankel. Through an investment company, Frankel succeeded at controlling a number of small insurance companies. He gained access to approximately $335,000,000. Because of his leadership position, Frankel was capable of circumventing internal controls. This enabled him to divert and embezzle over $200,000,000. When Frankel realized his fraud would be detected and law enforcement was closing in, he initiated his exit strategy. Frankel fled the United States and became a fugitive. He was ultimately arrested in Germany. Frankel also attempted to set fire to his two mansion compound in Greenwich, Connecticut. He maintained an office in the compound that contained his business and financial records. The intent of the fire was to destroy the records.

Fortunately, the mansions had sprinkler systems that extinguished the fire. At about the same time this occurred, FBI and IRS Agents showed up to execute a search warrant at the compound. One of the first items seized by an IRS Agent was Frankel's hand written to do list. The paper was singed from the fire and had water marks from the sprinkler. However, the hand writing was perfectly intact. Listed number one on Frankel's list was: launder money.

Five elements of fraud

Although the various types of fraud contain different characteristics and warning signs, they are all contingent on five common elements:

1. Integrity
2. Opportunity
3. Incentive, motivation or pressure
4. Rationalization or attitude
5. Capability

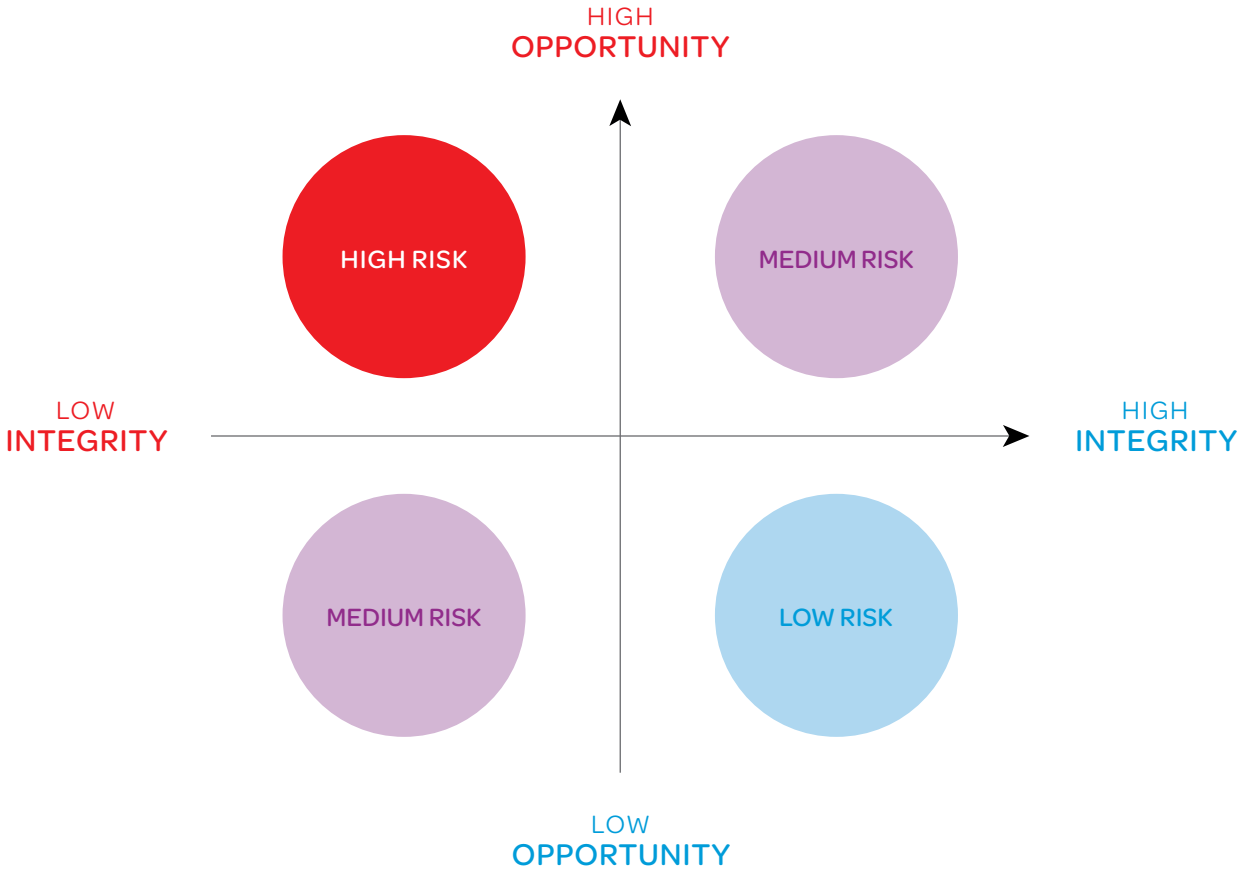
The starting point is individual integrity. Does a person have the integrity to resist opportunity? If yes, fraud is an afterthought. If a person's integrity is compromised, it's usually because pressure and rationalization lead that

individual to give into the enticement of opportunity. Opportunity is the driving factor. Without opportunity, a fraud scheme cannot succeed.

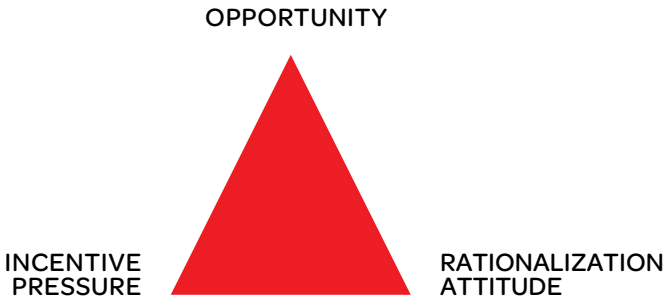
Likewise, if an individual's integrity is influenced by pressure and rationalization, and the opportunity presents itself, unless the individual possesses the capacity to commit the fraud, the scheme will not succeed. The capacity represents the combination of being in a position to commit the fraudulent act(s) and having the skill sets necessary to carry the fraud off.

The first step toward thinking like a fraudster is to understand how the five elements or fraud traits fit together to influence the bad guy.

The Fraud Continuum. I introduced the idea of the fraud continuum in the early 1980s, when I taught fraud awareness classes. The fraud continuum is the intersection between integrity and opportunity. The point of intersection of the two lines of the continuum creates four quadrants. The vertical line represents opportunity. The bottom of the line affords limited opportunity, while the top of the line represents a high level of opportunity. The horizontal line represents integrity. Limited integrity is on the far left side of the line and high integrity to the far right. The lower right quadrant represents where integrity is high and opportunity low. This is where people are least likely to engage in fraud. The upper left side of the quadrant is where opportunity is high and integrity low. This is where people are most likely to commit fraud. The other two quadrants represent moderate risk. This is where the combination of pressure, rationalization and capability most influence an individual's integrity.



The Fraud Triangle. The fraud triangle was introduced by Donald Cressey in 1973. The triangle consisted of three factors: opportunity, pressure and rationalization. These factors were long believed to be why individuals committed fraud. Opportunity is the chance to commit fraud. Pressure or incentive represents the motivation, and is usually driven by financial demands. Rationalization is the self justification making the fraudulent act acceptable.



The Fraud Diamond. The fraud diamond was introduced by David T. Wolfe and Dana R. Hermanson in 2004. Basically, they added a fourth dimension to the fraud triangle. Their reasoning was that unless a fraudster possessed the capability to commit a fraud, opportunity, pressure and rationalization by themselves were not enough to succeed. Capability required being in the right position at the right time and possessing the needed skill sets to perpetrate the fraud.

Harriette Walters, Matthew Kluger and Jeremy Blackburn did not know each other. They were all aspiring business professionals who had legitimate jobs and had experienced success. What did they have in common? At some point in time, each gave into opportunity and crossed the line of integrity and became fraudsters. Another commonality shared by these three strangers was the fact that they all went to jail.

Harriette Walters was a mid level supervisor in the District of Columbia, Office of Tax and Revenue. Walters recruited 10 co-conspirators and embezzled $48,115,419 over 18 years by causing 226 fraudulent property tax refund checks to be issued. Matthew Kluger was a mergers and acquisitions attorney. He provided inside information to two accomplices, who traded on, and illegally profited from, the inside information. Kluger and his partners netted over $32,000,000 in illicit profits. Jeremy Blackburn was the President of Canopy Financial, Inc. Blackburn and another Canopy executive defrauded investors out of $75,000,000 and misappropriated an additional $18,000,000 from custodial health care expense accounts.

Walters, Kluger and Blackburn identified opportunities in their respective schemes and compromised their integrity for greed (incentive) and entitlement (rationalization). They were in positions to commit fraud and possessed the necessary skill sets (capabilities) to succeed for a period of time. However, the burden of time created challenge for the fraudsters. Their ability to sustain the frauds diminished. As a result, the fraud schemes broke down and were detected.

Thinking like the bad guy

To think like a fraudster, you have to understand fraud on two levels, generic fraud and specific fraud:

Generic Fraud

In addition to understanding the five elements of fraud, you have to be familiar with what fraud is. Fraud encompasses an array of irregularities and illegal acts characterized by intentional deception. The elements of fraud include a representation about a material fact; which is false; and made intentionally, knowingly, or recklessly; which is believed; and acted upon by the victim; to the victim's detriment. The ability to be deceptive and avoid detection is one of the fraudster's primary keys to success.

Specific Fraud

Specific fraud is the type of fraud the bad guy commits. Building on the generic fraud principles, you have to understand how the specific scheme works, and how to exploit systemic vulnerabilities to facilitate your activity and perpetuate your scheme in order to avoid detection. Bad guys assess and identify mechanisms that enable them to perpetrate their schemes.

For example, investment fraud schemes have been prolific. They have been incredibly lucrative for the bad guys, while being extremely devastating to the victims. These schemes work because the fraudsters know how to entice their victims to invest in their deceptive offerings. The fraudsters also know how to use financial institutions to facilitate their fraudulent activity and provide them with a vehicle to launder their illicit gains.

Bad guys have the distinct advantage of being proactive, while industry and government are mostly reactive. They are motivated by the incentive of greed; they know what to look for, and how to manipulate the system.

What the bad guy looks for (opportunity)

Good fraudsters study the system and know the warning signs and risk factors to look for to provide them with the opportunity needed to commit fraud. They look for systemic vulnerabilities to exploit and adapt their plans to. Opportunities the bad guys look for within an organization include:

- Poor tone at the top
  - Weak ethical culture
- Lack of adequate internal controls
- Poor training
- Poor supervision
- Ineffective anti-fraud programs, policies and procedures

Fraud in motion

Once the bad guys identify opportunity, they have to fully understand the specific criminal activity they plan to engage in. Fraudsters consider variations of schemes that fit the situation and select the scheme that is least likely to be detected. They monitor and assess the scheme as it progresses and adapt it as necessary to continue to avoid detection. However a scheme is masked, involving a financial institution is essential. Proceeds from a fraud will have to be either directly deposited into an account or come into the account indirectly, through an intermediary. The bad guy must present the fraud and banking activity as being reasonable.

Reasonableness is a primary key to avoiding detection. This is where the bad guy must be deceptive and provide spin in the form of cover stories. This is the critical point of vulnerability for bad guys. Over time, spin and deception get much more difficult to disguise. The veneer of reasonableness tends to fade. A good fraudster usually watches intently for signs that their scheme is unraveling. At that point, they will implement their exit strategy. However, often times, fraudsters are blinded by their own greed and arrogance. They either miss or disregard the warning signs of detection. Instead of following an exit strategy, they find themselves in jail.

Case study

The book, Stolen Without a Gun illustrates the story of Walter Pavlo, Jr. It is an outstanding case study of how the elements of fraud work. This also highlights how bad guys think and take advantage of such opportunities as presented by poor tone at the top and lack of internal controls.

Pavlo started his business career as an honest, ambitious, fast rising junior financial executive at MCI Worldcom. The tone at the top was influenced by fraud and circumvention of internal controls. Worldcom's President, Bernard Ebbers, was ultimately convicted for a massive corporate fraud destroying Worldcom. Pavlo clearly had opportunity. However, early on, his integrity was not influenced by opportunity.

Unfortunately, that changed. Pavlo found himself in a position where he was pressured to "cook the books" by falsifying accounting records in order for Worldcom to make their quarterly projections. He dealt with unrealistic expectations, which caused him to "cook the books" on a recurring basis. The pressure of having to do this overcame Pavlo.

Pavlo became jaded and resentful about having to falsify financial records. He rationalized that he was underpaid and that everyone above him was cheating. Therefore, in his mind, it justified the implementation of a plan to embezzle company funds.

The pressure and rationalization Pavlo experienced led him to compromise his integrity and succumb to the opportunity to commit fraud. Pavlo had the capability to commit fraud because he was in a position to carry it out and possessed the requisite skill sets to do so.

Pavlo embezzled $6,000,000 from MCI Worldcom. His scheme fell apart when the broader corporate fraud, attributed to Ebbers, came to light. Pavlo was convicted and went to jail for his embezzlement scheme.

End game

Once you understand how to think like a bad guy, you can better position yourself to identify and investigate fraud schemes by breaking down spin and deception. Understanding the crime problem is the first step toward conducting a successful investigation. Good fraudsters usually have an exit strategy. When they realize their scheme has been, or will be, detected in the immediate future, they put their exit strategy in place. With that in mind, from an investigative stand point, you must have an end game. You don't want to see a fraudster disappear and abscond with the proceeds of their criminal activity.

There are two prominent end games. One has a private sector focus, the other, a public sector focus. On the private sector side, the end game is to prevent or minimize monetary losses and reputational risk. On the public sector side, it is to seek prosecution, recover illicit proceeds and assets through forfeiture, and/or bring enforcement actions. Both end games could carry significant consequences. In either event, understanding how the bad guys think and taking preemptive steps to stop them makes the end game easier to handle.

About the author

Dennis M. Lormel
President and CEO, DML Associates, LLC
www.dmlassociatesllc.com | Tel +571. 333. 0300

Dennis M. Lormel is a recognized subject matter expert in the anti-money laundering, terrorist financing, and fraud communities. Mr. Lormel is an accomplished speaker and is routinely engaged to provide training at industry conferences. In addition, he frequently participates in media interviews that reach both the U.S. and international markets. This exposure and his vast experience in the law enforcement and consulting fields have afforded him the opportunity to develop a unique and diverse network of colleagues and clients.

After the tragedy of 9/11, Mr. Lormel realized that the terrorists needed a financial infrastructure to accomplish the attacks. He immediately established an investigative organization within the FBI that, within days, identified the funding stream that supported these attacks. This is but one example of his expertise in assessing and establishing viable and effective recommendations that produce results.

In addition to Mr. Lormel's distinguished 31 year career in Government service, he has consistently delivered high quality consulting services to clients since 2004. The combination of law enforcement and financial services experience provides a comprehensive perspective on the issues that face individuals and corporate entities in today's complex world. Understanding the nexus between fraud and money laundering, especially on the heels of the financial crisis, allows Mr. Lormel to provide more comprehensive guidance to clients. The need for these services is increasing in the current economic environment.

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

Our financial services solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.