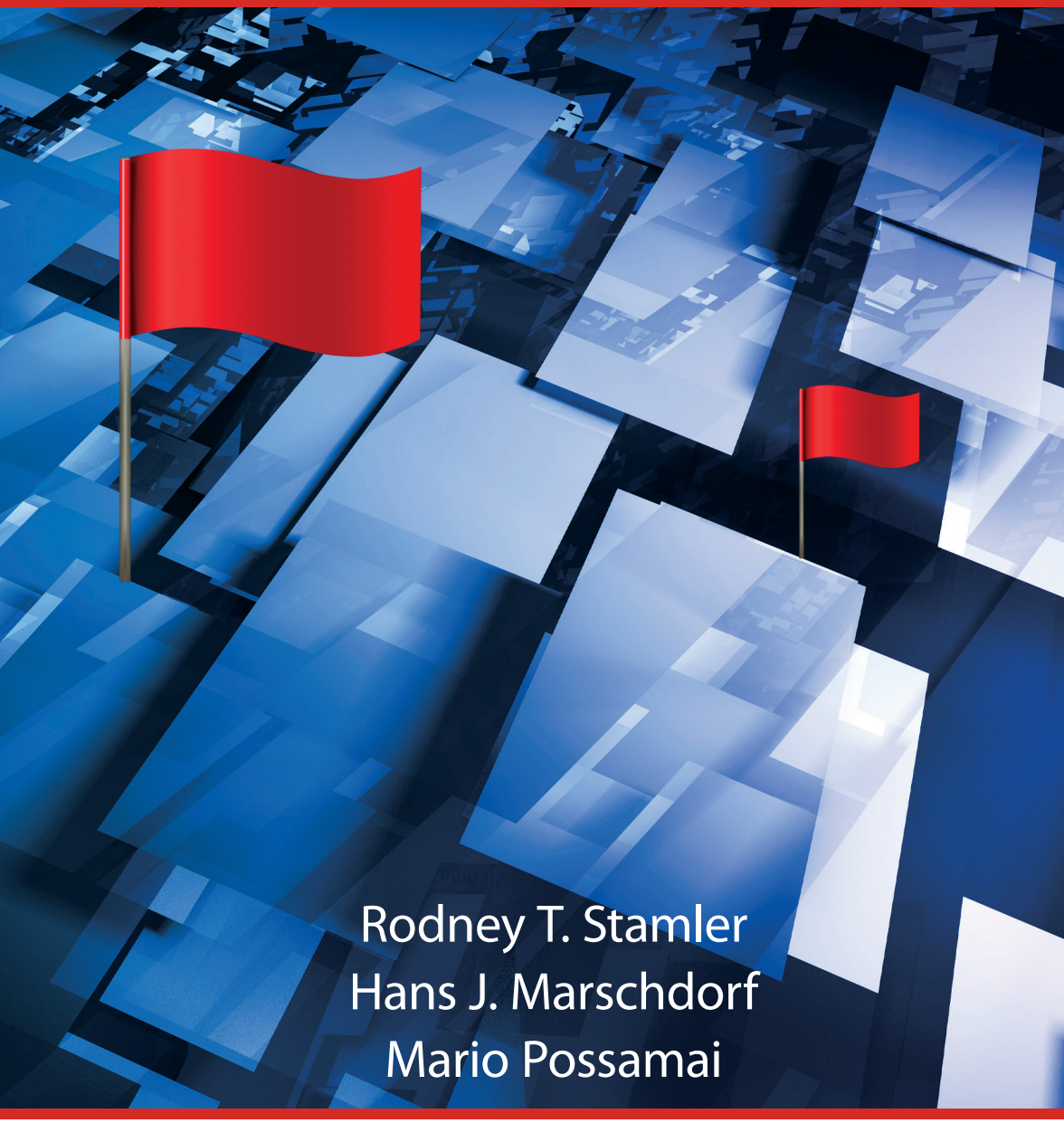
# Fraud Prevention and Detection

## Warning Signs and the Red Flag System



Rodney T. Stamler
Hans J. Marschdorf
Mario Possamai

CRC Press
Taylor & Francis Group

# Fraud Prevention and Detection

## Warning Signs and the Red Flag System

# Fraud Prevention and Detection

## Warning Signs and the Red Flag System

Rodney T. Stamler
Hans J. Marschdorf
Mario Possamai


CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742


Version Date: 20131112

International Standard Book Number-13: 978-1-4665-5455-9 (eBook - PDF)

# CONTENTS

# FOREWORD

Bob Lindquist, FCPA, CFE*

Over the past four decades, I have managed numerous cases around the world—cases involving a wide variety of domestic and international businesses and myriad fraud types.

Yet, there is a common thread running through virtually all of them: Red Flags. Before being discovered, just about every one of my cases had multiple indicators of fraud that, if addressed when first discovered, might have saved millions of dollars in losses and the untold pain that major frauds leave in their wake.

How to spot and take action on Red Flags in an effective manner is the subject of this book by Rod Stamler, Hans Marschdorf, and Mario Possamai.

It grew out of Rod's seminal work in the early 1990s, just after he retired from the Royal Canadian Mounted Police (RCMP) and joined my forensic practice. The Auditor General of Canada—roughly the Canadian equivalent of the US Government Accountability Office—had asked him to prepare a guidance document on how fraud can be detected much earlier in the fraud cycle.

As I write this, I am reminded of cases on which I worked with each of the three authors that had Red Flags at the core.

One that springs to mind involved a multinational computer manufacturer in the early 1990s. High-tech products can have a relatively short shelf life, which requires procedures to dismantle properly parts that are used, discontinued, or deemed to be surplus. Our client had chosen through the bid process to contract with various vendors to obtain this service with the agreement requiring the vendors to share their sale proceeds from recycled parts and not to sell parts scheduled for scrap. However, field investigators had found and confirmed the movement of the manufacturer's scrap in the "gray market" and our mandate was to determine if any person or group of persons within a certain division of the company was involved.

At the start of this matter, we met with the management in the division in question to advise of our investigation and to seek their cooperation.

* Robert T. Lindquist is the principal of Lindquist Forensics (www.lindquistforensics.com).

However, as we commenced, our primary subject of interest said he was too busy to be interviewed.

Now think about this: If he were honest he would have given me all the time I required. So I knew that his evasive behavior was a Red Flag, but now I had to establish the trail of evidence. Then, during an employee interview on the third day, a summary schedule of vendor bid prices was provided. A quick study of the document spoke "rigged bid." Several characteristics of a rigged bid were evident on this one piece of paper—an example of fraud knowledge or "Red Flags" at work.

Another case involved corruption and procurement fraud in the late 1990s in the construction of the international airport in the Republic of Trinidad and Tobago in the Caribbean. In one instance, 2 days before a contract was to be awarded, the requirements were changed and only two companies could meet the new requirements on time. It ended up being a winner pays loser scheme of procurement manipulation.

These cases had "Red Flags" written all over them. If these fraud indicators had been captured and acted upon earlier in the fraud cycle, our clients might have saved tens of millions of dollars in losses and prevented damage to their reputation.

There are many fraud books and articles aimed at accountants, auditors, and financial investigators—individuals whose professions have a fraud orientation. Increasingly, however, officers and directors in small, medium, and large companies; public agencies; nonprofits; charities; and foundations—individuals who usually do not have a fraud background—are being asked to take a leadership role in the prevention and detection of fraud. This book is intended to help the directing minds of public and private sector organizations—as well as their stakeholders—to know how to do so in an effective, efficient, and timely manner.

I believe that, in many cases of major corporate frauds, these disasters might have been averted—or at least their full impact diminished—if their boards had screened for Red Flags and taken action accordingly.

Readers of this book will acquire a general awareness of the nature, characteristics, and dynamics of fraud. They will also learn the process for determining whether a fraud has been committed. But, most importantly, they will learn how to find and take action on Red Flag indicators of fraud or suspicious transactions in financial statements, budgets, and contracts.

# THE AUTHORS

**Rodney T. Stamler** is a former assistant commissioner of the Royal Canadian Mounted Police (RCMP), who originated the "Red Flag" fraud detection and prevention system at the heart of this book in the early 1990s during an engagement with the Auditor General of Canada. Rod, who holds a law degree, perfected that system as a partner in two international forensic firms in the 1990s and into the early 2000s. His major cases included chasing the hidden assets of the late Romanian dictator Nicolae Ceausescu in the early 1990s; investigating the $1 billion Bre-X mining scandal in Indonesia, the world's largest gold mining fraud; and investigating a massive, multinational procurement fraud at a Fortune 100 multibillion-dollar corporation. During his career in the RCMP Rod was known as an innovator who was instrumental in establishing the crime program. He served as a special advisor to the United Nations in the development of the international convention against laundering the proceeds of illicit drug trafficking. He was formerly a member of the board of directors and member of the audit committee for a multinational mining company. Rod is often called to provide advice and counsel on corporate governance matters.

**Hans J. Marschdorf** is a leading international forensic accountant who has conducted financial investigations for the past 23 years around the world, ranging from multinational corruption and procurement fraud investigations to money laundering investigations, investigations of elaborate Ponzi schemes, and frauds involving structured financial products. His experience includes a position as pan-European leader of a forensic services practice in a Big 4 professional services firm. Mr. Marschdorf, a dual citizen of Canada and Germany, now practices as a financial crime investigator from Greater Toronto, Ontario (www.marschdorf-forensics.com). He holds a PhD in business administration from the University of Cologne, Germany, and is admitted to practice accounting in the European Union and Switzerland. He holds the designation of certified fraud examiner in the United States and chartered director in Canada. Mr. Marschdorf has published a number of articles on aspects of fraud investigation and corruption, economic analysis of insolvency law, and international taxation.

He serves as chairman of the advisory board of the School of Governance Risk and Compliance of Steinbeis Hochschule, a Berlin business school, and is also a member of its faculty.

**Mario Possamai** is a senior fraud professional at a major Canadian financial institution and has managed complex fraud, asset recovery, and corruption investigations in North America, Europe, and Africa for more than two decades. A member of the Bre-X investigative team in Indonesia, Mario also provided forensic financial consulting services to the director of public prosecutions in a southern African country in the mid-1990s; was an expert witness for the Department of Justice in Canada on money laundering; and was senior advisor to Superior Court Justice Archie Campbell, who headed the judicial inquiry into the SARS outbreak in 2003. He is the author of a book on money laundering and for 10 years was a guest lecturer at the Financial Fraud Institute at the US Department of Homeland Security's Federal Law Enforcement Training Center in Glynco, Georgia.

# 1

# *An Introduction to the Red Flag System*

## A PERSISTENT THREAT

No entity is immune from fraud. Fraud indiscriminately affects all types of organizations regardless of sector, size, or geographical location. It does not distinguish between public or private entities, by what they do, by their environmental footprint, by their level of sustainability, by their public profile, or by the number of years they have been in existence. It is not softhearted: Nonprofits or charitable entities are potentially just as vulnerable to fraud as those focused on making profits. They may, in fact, be more vulnerable because they may not be able to afford more sophisticated controls or cannot afford to allocate sufficient resources to fraud prevention and detection.

Consider the following:

- A study by the Association of Certified Fraud Examiners (ACFE) estimated that a typical organization loses 5% of its revenue to fraud each year. The data for this study involved more than 1,300 cases in 100 countries.[*]
- A global survey by PriceWaterhouseCoopers (PwC) found that 34% of respondents had experienced a fraud in the previous 12 months. This survey involved 3,877 respondents around the world.[†]

[*] Association of Certified Fraud Examiners. 2012. Report to the nations on occupational fraud and abuse: 2012 Global fraud study, Austin, TX.

[†] PWC. 2011. Global economic crime survey, London: November 2011.

- The Kroll Global Fraud Report reported that six of ten companies surveyed had been affected by fraud in the previous year. This was based on a survey of nearly nine hundred senior executives worldwide.*

Fraud is costly in many ways:

- The median loss in the aforementioned ACFE study was $175,000 and more than one-fifth of the frauds analyzed involved losses of at least $1 million.†
- In the previously noted PwC study, one in ten suffered losses of more than $5 million.‡

But financial losses are just part of the adverse consequences of fraud. How a company deals with fraud says a lot about it and provides strong signals to stakeholders, employees, clients, vendors, shareholders, and regulators:

- How strong are its internal controls? Are they easily circumvented?
- Does it have a lackadaisical culture, where no one seems to care? Or is it a culture that does not tolerate fraud and other improprieties?

Recent research indicates that a significant proportion of a company's value (potentially over 60%) relates to intangible assets like reputation.§ While its precise contribution to a company's worth is difficult to quantify, there is no doubt that reputation has significant economic value¶ since reputational damage can adversely impact brand value and share price, including new financings.

---

* Kroll Advisory Solutions. 2012. Global fraud report 2012/2013, New York: October 2012.

† Association of Certified Fraud Examiners. 2012. Report to the nations on occupational fraud and abuse.

‡ PWC, Global economic crime survey.

§ Nick Rea and Adrian Davis. 2005. Intangible assets: What are they worth and how should that value be communicated? Published in *IP Value* 2005, Building and enforcing intellectual property value.

¶ Dr. Baruch Levy of the Stern School of Business in New York defines the economic value of reputation as follows: "It is a seller's guarantee or commitment of contracted performance and product/service quality. Accordingly, the benefits to the owner of reputation are the premia paid by the counterparty (customers, employees, suppliers, investors) for the guarantee. The value of reputation, and its share in the market value of the company is the discounted value of the expected premia stream, net of the cost of maintaining reputation. Reputation is the outcome of a credible guarantee/commitment." Source: Baruch Levy. 2005. The art and science of valuing intangibles and managing reputation (or: The confession of a heartless economist), New York University, baruch-lev.com, September 2005.

A good reputation (and its contribution to an organization's value) can be quickly lost, sometimes overnight, if not properly managed. Significantly, reputation, as one author noted, "…is most at risk during a critical major event."*

An Oxford University study says companies that effectively manage critical incidents, like the public disclosure of a major fraud, gain market value, while the shares of ineffective ones can lose a lot of value. The study found that corporations lost an average of 15% in net stock value in the months following an ineffective response to a large-scale emergency. An effective response increased companies' total market value by about 22%.†

Reputation is especially important for nonprofits and charities that rely on government funding and individual or corporate donations:

- Donors may have second thoughts about giving to a charity that is vulnerable to fraud. They may have doubts about whether their donations are actually being used for their intended purpose.
- Trust in a community hospital may be eroded by a fraud, causing stakeholders to wonder whether there is sufficient oversight in other areas, like patient care and safety.
- Fraud against a school board can tarnish its reputation among parents, students, and teachers.
- Fraud committed against a religious institution can negatively impact its ability to carry out its charitable works and can cause rifts among its members and stakeholders.

Fraud can also dampen employee morale and create recruiting and retention problems. How would you feel if a fraud against your employer was splashed across the media? How would you answer related questions from neighbors, family, and friends?

Many lawsuits have been launched in recent years against directors and officers who failed to protect their companies sufficiently from fraud. Taking a proactive approach to fraud prevention and detection could help protect officers and directors from the consequences of having a major fraud erupt on their watch.

Moreover, if you are trying to attract strong candidates to your board or executive ranks, the fact that you have an effective, proactive system

* Bexon Brohman & Associates. 2007. Board oversight doesn't stop at the buck. January 24, 2007.

† Rory F. Knight and Deborah J. Pretty. 1996. The impact of catastrophes on shareholder value. Published in 1996 as part of the Oxford Executive Research Briefings, Templeton College, Oxford University.

for preventing fraud also can make your organization more attractive and enhance your recruitment efforts. Imagine that you are a strong candidate considering joining a company that has just become the victim of fraud. Would you not have second thoughts about such a move? The prospective candidate can take comfort that your organization is doing all it can to help directors and officers properly discharge their antifraud responsibilities and thus maintain their personal reputations.

Fraud can also cause major financial damage if committed by the corporation. Prominent examples relate to violations of bribery laws by large corporations and manipulations of procurement processes for the financial gain of such corporations. The list of enforcement actions by regulators in the United States, the UK, and Canada in bribery cases is impressive and includes violations by such large international corporations as Halliburton and KBR, Siemens, and DaimlerChrysler, to name just a few.*

The damage, again, is reputational, but the penalties and procedural costs can amount to several billion dollars. Former US Deputy Attorney General Paul McNulty in a keynote address famously stated: "If you think compliance is expensive, try noncompliance."†

## THE RED FLAGS OF FRAUD

When it comes to fraud, there is no silver bullet—no single, magical solution. However, there are prudent measures that can help reduce the risk of fraud and increase the chances that it can either be prevented or detected much earlier.

Based on their more than 100 years of combined experience in the investigation and prevention of fraud in North America, Europe, and the Far East, the authors set out a structured approach—known as the Red Flag System—for the prevention, early detection, and appropriate investigation of fraud.

The Red Flag System is practical, effective, and empirically tested. It is based on the premise that to prevent fraud successfully or detect it as quickly as possible after it begins, an organization must have the capacity

* For a complete list of US enforcement actions from 1978 to 2012, see http://www.sec.gov/spotlight/fcpa/fcpa-cases.shtml (accessed July 23, 2013).

† Compliance Week Conference. 2009. http://www.compliancebuilding.com/2009/06/04/mcnulty-keynote-on-a-tale-of-two-sectors/ (accessed July 23, 2013).

to identify, analyze, and address possible indicators of fraud, known as "Red Flags," in a timely manner. "Red Flags" are like the first wisps of smoke in a forest. Detect them early enough and you can prevent a forest fire. Fail to move decisively and the whole forest may be in danger.

The Red Flag System can be especially beneficial for corporate officers and directors.

To understand the Red Flag System, keep in mind that frauds do not come out of the blue, and they do not happen overnight. They are not random one-off events. According to a study by the ACFE, the typical fraud lasts 18 months from the time it begins until it is discovered.* Some frauds stay undetected even longer.

For example, fake billing cases—in which payments are made for fictitious goods and services or invoices are inflated—may be undetected for 24 months.† Cases of ghost employees being added to the payroll take even longer to spot—as long as 36 months.‡

Consider what occurs over the life cycle of a fraud. The perpetrator may begin small but over time may perfect his or her skills so that larger frauds can be executed. A trusted bookkeeper, for example, may start by creating—and then paying—fake invoices to cover some overdue bills. The bookkeeper tells herself that this will never happen again. But little by little she gets hooked on the easy money. Over time, the bookkeeper also gets better at concealing her fraud. But somewhere along the way she would have created some Red Flags—indicators that something was amiss. If those Red Flags had been investigated, the fraud would have been stopped sooner.

Over the time frame of a fraud, there are usually Red Flags—indicators that something was amiss. And this aspect of fraud is precisely what is at the heart of the Red Flag System. Some examples include:

- A procurement fraud may have been heralded by the decision of a manager to get rid of established vendors in favor of smaller, less well-known suppliers. The manager might have claimed that this would save money and eliminate red tape. In fact, he was in collusion with a crime group that jacked up the cost of inputs. His scheme might have been halted if the decision to get rid of established vendors had been more deeply and rigorously investigated;

* Association of Certified Fraud Examiners. 2012. Report to the nations on occupational fraud and abuse.
† Ibid.
‡ Ibid.

- A trusted bookkeeper dresses in the latest fashion and drives a luxury foreign sedan, telling everyone she had consistently done well at the local casino. In fact, she had created a dozen ghost employees and pocketed the proceeds. This scheme might have been cut short if someone had delved more deeply into how she had been able to afford this lifestyle;
- The chief financial officer (CFO) of a multinational mining firm recommended getting rid of a national auditing firm and hiring a small, two-person firm with an office in a suburban strip mall with no experience in the extractive sector. It was just a smart way to save money, the CFO told the board. In fact, the small audit firm conspired to help the CFO manipulate the accounts and perpetrate a financial statement fraud. A more aggressive scrutiny by officers and directors might have stopped this scheme in its tracks.

According to both fraud research and the coauthors' experience, the problem is that Red Flags often are either not captured or, if they are, they are not appropriately investigated in a timely manner.

Some of the research in this area has been done by the Big Four internationally operating accounting firms, PwC, KPMG, Ernst & Young, and Deloitte. A study by KPMG found that there had been signs of fraud in 45% of major fraud cases analyzed. However, in only one in four cases had the company investigated the Red Flags.* When KPMG looked at this issue again 4 years later, it found that 56% of the 348 major fraud cases analyzed were heralded by Red Flags. However, only 6% of Red Flags were acted upon.†

Why are fewer and fewer entities capturing and pursuing Red Flags?

In part this is because officers and directors are often under the mistaken view that laws, regulators, and law enforcement will protect them from fraud.

A key lesson can be drawn from major frauds. Whether the victim is a company, a public agency, a nonprofit, a foundation, or a charity, there was a higher likelihood that many frauds could have been prevented or detected earlier if Red Flags (i.e., the early warning signals that are the focus of this book) had been taken seriously.

But in the authors' extensive experience, officers, directors, and stakeholders also frequently do not know how to identify, analyze, and take action on "Red Flags." Their concentration is usually on building their

* Released in 2011, KPMG Analysis of Global Patterns of Fraud is based on an analysis of 348 actual fraud investigations in sixty-nine countries.

† Ibid.

business—not on how to safeguard it against fraud. They may have "blind spots" regarding employees in positions of trust who may be known to "cut corners" in the company's best interest.

To prevent and detect fraud effectively, entities must be able to identify, analyze, and take action on Red Flags in a timely manner. As noted before, ignoring these early warning signals of potential frauds or not investigating them appropriately risks allowing a fraud to take root or, in a worst-case scenario, to persist unseen.

The adverse effects on the bottom line, on an entity's ethical framework, and on officers'/directors' personal liability can be considerable.

To be sure, the Red Flag System is not a magic bullet. It is not a guarantee that you, your company, your foundation, or your charity or other public and private entity will not be a victim of fraud. But it will provide you with the tools to address the fraud challenge more effectively and be in a better position to detect a fraud earlier in the fraud cycle.

## DEFENSE IN DEPTH

The Red Flag System is not a stand-alone defense against fraud. Rather, its effectiveness requires an integrated fraud prevention and detection strategy. It is a bit like the alarm system in a building. You cannot just install an alarm system and hope that it is enough to keep out intruders. You need trained staff to monitor the system and appropriately investigate alarms, including differentiating between false alarms and incidents that warrant investigation. You need appropriate entry and exit systems so that only employees can enter the building and access areas relevant to their jobs and responsibilities.

Ultimately, you need what security experts call "defense in depth":

> The concept of defense-in-depth…involves concentric rings of protection that utilize the physical structure of a location to block or impede the progress of burglars towards their targets, as well as making it more difficult for them to exit with stolen property. Layers of security should serve to initially deter intruders. Where this fails, delays at each stage should allow sufficient time for a detection system to alert an appropriate guardian who can intercept the intruder.*

* Tim Prenzler, PhD. 2009. Preventing burglary in commercial and institutional settings. ASIS Foundation, Arlington, VA.

Similarly, with the Red Flag System, to function effectively, the system needs to be anchored within policies, procedures, and systems that comprise an effective fraud defense in depth. These include:

- A strong ethical culture, including setting the right tone at the top—the lack of ethical behavior by an organization's leaders can percolate down throughout an organization, creating an environment where employees are more likely to engage in fraudulent activities
- Effective internal controls* that reduce a fraudster's ability to perpetrate his or her schemes, and avoid early detection and investigation
- The presence of detection systems, including fraud analytics and audits, to foster an environment in which a potential fraudster is aware that his or her chances of detection are significant
- Employee education in fraud detection and prevention
- Hotlines for employees to report unusual activities safely without fear of retribution

Conversely, it is important to ask yourself the following questions:

- Does my entity have a strong ethical culture?
- Does it have strong and effective internal controls, whose presence is validated by outside auditors?
- Are there effective detection systems?
- Are employees educated in fraud prevention and detection?
- Are there hotlines for employees to report unusual activities?

If you answer "no" to one or more of these questions, your organization may have a heightened vulnerability to fraud.

By having an effective fraud defense in-depth program, Red Flags can be effectively captured, analyzed, and action taken in a timely manner. However, it is important to note that, on their own, internal controls and the other elements of a fraud defense in-depth program are not enough and can even create a false sense of security without a dynamic proactive approach like the Red Flag System.

---

* "Internal controls are put in place to keep the company on course toward profitability goals and achievement of its mission, and to minimize surprises along the way. They enable management to deal with rapidly changing economic and competitive environments, shifting customer demands and priorities, and restructuring for future growth. Internal controls promote efficiency, reduce risk of asset loss, and help ensure the reliability of financial statements and compliance with laws and regulations." Source: The Committee of Sponsoring Organizations (of the Treadway Commission); see http://www.coso.org/publications/executive_summary_integrated_framework.htm

An organization's internal controls, for example, may appear sound and comprehensive, but they may not be oriented to the prevention and early detection of fraud.

A case in point involved the giant French bank Société Générale, which discovered a $7.2 billion fraud. It appears that Société Générale's internal controls were, in themselves, effective, identifying nearly one hundred operational anomalies, or Red Flags, over a 2-year period. The problem appears to have been that no one took notice. No one followed up by rigorously analyzing these anomalies in a timely manner—a fundamental feature of the Red Flag System.

As the *Wall Street Journal* reported: "Société Générale SA's $7.2 billion loss on a series of fraudulent trades is just the latest example of a breakdown in internal controls that are supposed to protect financial firms from disaster."[*]

## CAN YOU RELY ON REGULATORS OR LAW ENFORCEMENT?

Perhaps at greatest risk of fraud are organizations that believe law enforcement and regulators can protect them. Consider the following quote: "The things he was able to do in carrying out his swindle would never again be possible, and in that sense he may also be said to have been the last of a free-wheeling breed."[†]

This could have been written about the masterminds behind the Enron,[‡] Bernie Madoff, Tyco International,[§] and WorldCom[¶] scandals. In fact, it referred to Ivar Kreuger, a notorious 1930s Swedish financier who was dubbed "the world's greatest swindler."

---

[*] *Wall Street Journal*. Once again, the risk protection fails, January 25, 2008.

[†] *The Economist*. The match king, December 19, 2007.

[‡] Based in Houston, Enron Corporation had been one of the world's top energy traders until revelations in 2001 of institutionalized, systematic accounting fraud. It filed for bankruptcy protection in late 2001.

[§] Incorporated in Bermuda, Tyco International was a rapidly expanding conglomerate that fell victim to accounting scandals in 2002. In 2005, its former chief executive and his top lieutenant were convicted of fraud. In 2007, the company agreed to pay almost $3 billion to defrauded investors, the largest ever such payment.

[¶] Based in Clinton, Mississippi, WorldCom was a telecommunications giant that filed for bankruptcy protection in 2002 following the disclosure that fraudulent accounting methods had been used to conceal declining earnings.

His securities—issued in small denominations and paying annual dividends of more than 20%—had been the most widely held in the world. Unfortunately, the dividends came from capital, not profits. This created "a giant pyramid scheme, which was hidden from the investing public by Kreuger's insistence that financial statements not be audited."* When the scheme crashed in 1932, the resulting bankruptcy was the largest on record and helped lead to the passage of the landmark US securities acts in 1933 and 1934.†

Big financial scandals like Kreuger's or those involving Madoff, Enron, Tyco International, and WorldCom are nothing new. They have been around for a long time and we have not seen the last of them.

As occurred in the early 1930s, after the dot.com bubble at the start of the twenty-first century and after the global meltdown in 2008, major frauds invariably cause lawmakers to try to close the loopholes the scandals exposed. Modern history is full of such legislative hand-wringing.

Unfortunately, the new regulatory regimes are more suited to fighting the last war instead of the next one. They may address the fraud still fresh in everyone's mind, but will not necessarily stop other types of fraud.

It is similarly not prudent to believe that law enforcement will protect you and your entity from fraud. To be sure, there are many cases where law enforcement is able to stop a fraud in progress. But while there are some successes, they are usually in frauds that have reached a critical point. An example was the epidemic of mortgage fraud and Ponzi schemes that came to light after the 2008 financial crisis.

As Michael J. Byrne, chief counsel of the Pennsylvania Securities Commission, has noted:

> These schemes collapse because ultimately they lose their credibility and thus their ability to recruit the new investors necessary to maintain performance of the outstanding promises. With regard to Madoff, Warren Buffett's aphorism is instructive, "When the tide goes out you learn who is not wearing a bathing suit." In other words, you learn who does not have the funds necessary to perform their outstanding promises. The turmoil in the market resulting from the [2008] financial

* Dale L. Flesher and Tonya K. Flesher. 1986. Ivar Kreuger's contribution to US financial reporting. *Accounting Review* LXI (3), July 1986.

† "These two acts required companies to publish audited financial statements before selling securities to the public and established the Securities and Exchange Commission to oversee corporate financial reporting." Source: Paul M. Clikeman. 2003. The greatest frauds of the (last) century. Robins School of Business, University of Richmond, Virginia, May 2003.

> meltdown caused an unprecedented number of Madoff's investors to decide to leave the stock market for safer havens. Madoff could not raise the funds necessary to cover the increasing demands for redemptions.[*]

Law enforcement is more typically reactive than proactive. It usually responds to complaints. It has neither the resources nor the mandate to act as a guardian angel to detect and prevent fraud.

The bottom line: History shows that you cannot rely solely on laws, regulators, or law enforcement to prevent fraud because white-collar criminals invariably find a way around those barriers. It almost goes without saying: When it comes to compliance violations, your goose is already cooked when law enforcement knocks on your door. This places the officer or director of a company or a nonprofit in a difficult position:

- On the one hand, he or she has a fiduciary duty[†] to safeguard the organization's assets and reputation from fraud.
- On the other, the officer or director takes on this huge responsibility even though he or she usually is not trained in fraud prevention and detection or was not primarily hired for this purpose.

In most instances, fraud prevention and detection were likely the last thing on the officer's or director's mind when he or she accepted this position.

So what can you do to protect yourself and your organization against fraud?

Based on our decades-long experience, we have come to the conclusion that prudent corporate officers or directors would implement the Red Flag System for the prevention and early detection of fraud. It is practical, effective, and empirically tested. It is based on the premise that to prevent fraud successfully or to detect it as quickly as possible after it has begun, an organization must have the capacity to identify, analyze, and address possible indicators of fraud, known as "Red Flags," in a timely manner.

Red Flag fraud detection requires skills and expertise that are outside the normal duties and practices of those who manage and run organizations. Under normal circumstances, most people in an organization, from the chairman of the board to the members of the Audit Committee to the internal auditors and the external auditors, have not been selected because of their ability to detect fraud.

---

[*] http://www.legis.state.pa.us/cfdocs/legis/TR/transcripts/2009_0157_0001_TSTMNY.pdf (accessed July 23, 2013).

[†] "The duties of a fiduciary include loyalty and reasonable care of the assets within custody. All of the fiduciary's actions are performed for the advantage of the beneficiary." Source: *West's Encyclopedia of American Law*. Copyright 1998 by The Gale Group, Inc.

Unlike police organizations, regulatory agencies, and accounting firms, which have specially trained fraud investigators or forensic accountants, most people are hired or invited to join an organization as director or hired as an officer to further its objectives.

The Red Flag System helps directors and officers to discharge their responsibility to prevent and detect fraud, even though they are not fraud investigative specialists.

Red Flag fraud detection also requires a thought process outside the usual practices of financial review and audit. Financial auditing relies on generally accepted auditing standards to express an opinion on financial statements based on the audit. It is not primarily intended to detect the Red Flags of fraud.

Rather, a financial audit is based upon a structured step-by-step approach whose objective is to find material errors and irregularities in either the financial statements or in the appropriate handling of revenues, investments, and assets. Financial auditing is not designed to detect all errors, irregularities, and fraud since it is based on sampling techniques that are driven by the accounting concept of materiality.* Finally, such audits are always subject to budget or fee restrictions.

A fraud investigation is not a checkbox exercise. Often its progress and direction depend on professional judgment applied to findings as they develop. The findings usually arise from the analysis and further investigation of one or more Red Flags that initially suggested the potential for fraud.

## ABOUT THIS BOOK

This book sets out a no-nonsense approach known as the Red Flag System for the prevention and early detection of fraud. It reflects the coauthors' more than 100 years of combined experience in the investigation and prevention of fraud in North America, Europe, and the Far East. The authors have included cases, laws, and regulations from a number of different

* "Accounting information is considered material if its deletion or misstatement would alter or affect the judgment of any reasonable individual relying on the information. Materiality, therefore, guides accountants in determining which accounting information should be disclosed." Source: Kenneth J. Fowler. 1993. Quantitative guidelines: Guidance based on professional pronouncements. *CPA Journal*, March 1993.

countries and jurisdictions, in order to give the reader a more international perspective in dealing with corporate fraud and corruption.

Many people can benefit from this book. It will help officers and directors fulfill their fraud prevention and detection responsibilities and duties. While they have a fiduciary duty to safeguard their organization against fraud, officers and directors may not be trained or experienced in fraud prevention and detection. At any rate, this is not likely why they were hired or appointed in the first place, though there is an expectation that they can help safeguard their entity from fraud. This book will help them to discharge their responsibilities, even though they are not fraud investigative specialists.

But it will also be useful to others as well, including:

- Shareholders so that they can better monitor the companies in which they have investments
- Managers and supervisors who want to improve their business units' and departments' fraud prevention and detection capabilities
- Union leaders and members interested in keeping an eye on the antifraud effectiveness of their employers
- Journalists who cover business and financial matters
- Regulators
- Stakeholders in charities, foundations, and other entities in the not-for-profit sector

Readers of this book will:

- Acquire a general awareness of the nature, characteristics, and dynamics of fraud
- Understand the process for determining whether a fraud has been committed
- Develop an understanding of enterprise risk management approaches for fraud risk management, compliance risk management, and managing the risk of fraudulent financial reporting, including an understanding of the limitations inherent in these approaches
- Learn how to find Red Flag indicators of fraud or suspicious transactions in financial statements, budgets, and contracts
- Know how to ensure that, once a Red Flag has been identified, appropriate action is taken

Moreover, this book is designed to:

- Increase the general awareness of the possibility of fraud that may be committed by management and employees or by third parties who are carrying on business with an organization
- Describe the changing role and responsibility of directors and committee members who have the responsibility to examine and approve financial statements, budgets, and contracts
- Help to understand how to look for and identify fraud by identifying Red Flags as an indicator
- Increase awareness of how to conduct the examination required to detect and scrutinize Red Flags
- Outline how to examine individuals that are presenting financial documents for approval
- Describe how to report when a Red Flag has been identified
- Outline how to coordinate the various internal and external systems that may be utilized to investigate Red Flags
- Review the roles of lawyers, auditors, forensic accountants, public officials, and other experts that may become involved in the Red Flag investigation
- Ensure that as a member of a board of directors or a board committee you will not be included as a party or conspirator to a civil or criminal charge that may result because of negligence on the part of the board, the committee, or certain of its members