CHAPTER ONE

1

Introduction to Occupational Fraud and Corruption and Recent Trends

WHEN I STARTED WRITING THIS BOOK, I considered jumping in at the deep end and commenced rapidly making notes of the various approaches to profiling by compiling a list, based on my 20 or so years of experience in the fraud investigation field, of exactly what, when profiled, would be of use to the fraud investigator. Yes, there is the behavior of the convicted fraudster to understand as well as his modus operandi, but what about which industry type or department he is likely to work in, his likely position within the organization, the likely geographical location, economic environment, and personal circumstances? We also need to understand the profile of higher risk victim organizations and their characteristics. Anyway, I quickly realized that to fully understand the subject of profiling we first need to have a fairly good grounding in or understanding of the subject of fraud and corruption—what it is and how it affects organizations and all of us who are associated with those organizations. It is also, possibly even more so, very important to understand the types of controls that are designed, put in place, and often bypassed to enable us to manage fraud risk in organizations. After all, fraud is perpetrated by human beings as a reaction to opportunities created by weak safeguarding processes. Profiling is a further antifraud methodology to add to the stable, and it does require an understanding of how and where in the

corporate environment it would best sit. After all, you would not bring in a new team member without first ensuring a good fit or put a new thoroughbred into a stable to share with other horses without first having an understanding of those neighbors and what makes them kick. So, let's have a look at the world of fraud and corruption and how, since time immemorial, we appear to be failing in our attempts to manage fraud risk in the organizational environment.

DECEPTION THROUGH BREACHING TRUST

The term *fraud* has come to encompass many forms of misconduct. Although the legal definition of fraud is very specific, for most people like you and me, antifraud professionals, regulators, the media, and the general public alike, the common use of the word is much broader and generally covers any attempt to deceive another party to gain a benefit. Expense fraud, forgery, counterfeiting, identity theft, theft of inventory by employees, manipulated financial statements, insider trading, Ponzi schemes, mortgage fraud—the range of possible fraud schemes is actually endless but at their core all involve a violation of trust. It is this violation that, perhaps even more than the resulting financial loss, makes such crimes so harmful. For businesses to operate and for commerce to flow freely, organizations must entrust their employees with resources and responsibilities. So when an employee defrauds his or her employer, the fallout is often especially harsh. The focus of this book is *occupational fraud* schemes in which an employee abuses the trust placed upon him or her by an employer for personal gain. The formal definition of *occupational fraud*, taken from the Association of Certified Fraud Examiners (ACFE) website, http://www.acfe.com/fraud-101.aspx is

> the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets.

While this occupational fraud category is but one facet of the vast overall fraud universe, fraud in the workplace is huge and covers a wide range of employee misconduct. It is, without doubt, a material threat faced by all organizations and their employees worldwide.

GLOBAL TRENDS IN OCCUPATIONAL FRAUD

The Association of Certified Fraud Examiners (ACFE), a leading professional body of fraud examiners, has undertaken extensive research into the costs and

trends relating to occupational fraud schemes. The findings of the ACFE's initial research efforts were released in 1996 in the first *Report to the Nations on Occupational Fraud and Abuse*, with subsequent reports released in 2002, 2004, 2006, 2008, and 2010. The ACFE's 2012 *Report to the Nations on Occupational Fraud and Abuse*, now carried out every two years, provides an analysis of 1,388 fraud cases investigated worldwide by qualified fraud examiners and continues a tradition of shedding light on trends in the characteristics of fraudsters, the schemes they perpetrate, and the organizations being victimized. The ACFE findings truly reflect global trends in occupational fraud and abuse and are invaluable in keeping us abreast of the fraud disease.

The goals of these reports have been to

- Summarize the opinions of experts on the percentage of organizational revenue lost to all forms of occupational fraud and abuse.
- Categorize the ways in which occupational fraud and abuse occur.
- Examine the characteristics of the employees who commit occupational fraud and abuse.
- Determine what kinds of organizations are victims of occupational fraud and abuse.

Each version of the report has been based on detailed information about fraud cases investigated by certified fraud examiners (CFEs). Each new edition expands and modifies the analysis contained in the previous reports to reflect current issues and enhance the quality of the data that is reported. This evolution has allowed the release of increasingly meaningful information from the experiences of CFEs and the frauds that they encounter.

Fraud, like many other crimes, can be explained by the existence of the following four key drivers:

1. A supply of motivated, pressurized, or incentivized offenders.
2. The absence of capable guardians and policing, or weaknesses in control systems, opening up an opportunity.
3. Rationalization in the fraudster's mind bringing about justification for his actions in exploiting the opportunity to satisfy the motivation.
4. The availability of suitable victim organizations.

The motivation, pressure, or incentive to defraud may be as simple as financial need or greed or anything from unrealistic deadlines and performance goals to personal vices such as gambling or drugs.

The opportunity to commit and conceal fraud is really the only element over which an organization has significant control. The opportunity is an

open door to solving a nonshareable problem by violating a position of trust and is generally provided through weaknesses in the internal controls. Some examples of weak internal controls include but are by no means limited to absent or inadequate procedures surrounding the following:

- Supervision and review.
- Segregation of duties.
- Management approval and delegation of authority.
- System controls.

Rationalization is a crucial component because most people need to reconcile their behavior with the commonly accepted notions of decency and trust. Some examples of justifications for their actions given by fraudsters I have met include the following:

- "I really need this money, and I'll put it back when I get my salary at the month's end."
- "I'd rather have the company on my back than the tax people."
- "Everyone else is doing it."
- "I just can't afford to lose everything I have worked for—my home, car, everything."

The availability of a suitable victim organization is an easy one. It is more often than not the fraudster's employer, with whom he has built up a relationship of trust, quite often over many years.

The ACFE 2012 *Report to the Nations on Occupational Fraud and Abuse* analyzes statistics from fraud cases investigated worldwide to gain an understanding of the characteristics of fraudsters, their schemes, and the types of organizations being targeted. Throughout the report, the statistics include comparison charts showing several years of data, which highlight the consistency of findings over time. This uniformity is among the most notable of observations from the ongoing research and indicates that the findings truly reflect global trends in occupational fraud and abuse and that the ACFE statistics represent an important core base for profiling in any organization.

THE COST OF OCCUPATIONAL FRAUD AND CORRUPTION

Determining the full cost of occupational fraud is an important part of understanding the depth of and motivation for the fraud problem. News

reports provide visibility to the largest cases, and most of us have heard stories of employees who have brazenly stolen from their employers. Even so, fraud is all too often treated as an anomaly in the business process rather than a common example of the risk faced by all organizations. Unfortunately, obtaining a comprehensive or exact measure of the financial impact of fraud and corruption on organizations is challenging, if not impossible. Because fraud inherently involves efforts of concealment, many fraud cases will never be detected, and of those that are, the full amount of losses might never be determined or reported. Consequently, any attempt to quantify the extent of all occupational fraud losses will be, at best, an estimate. As part of the ACFE's research in its *Report to the Nations*, each CFE who participated in the survey was asked to provide his or her best assessment of the percentage of annual revenues that the typical organization loses to fraud. The median response indicates that organizations lose an estimated 5 percent of their revenues to fraud each year. To illustrate the magnitude of this estimate, applying the percentage to the 2011 estimated gross world product of $70.28 trillion results in a projected global total fraud loss of more than $3.5 trillion. It is imperative to note that this estimate is based on the collective opinion of antifraud experts rather than on specific data or factual observations, and should thus not be interpreted as a literal calculation or extrapolation of the exact and total worldwide cost of fraud against organizations. Even with that caveat, however, the approximation provided by more than 1,000 CFEs from all over the world with a median 11 years of experience as professionals who have a firsthand view of the fight against fraud may well be the most reliable measure of the cost of occupational fraud available and certainly emphasizes the undeniable and extensive threat posed by these crimes.

Of the 1,388 individual fraud cases reported in the ACFE survey, 1,379 included information about the total dollar amount lost to fraud, as shown in Figure 1.1.

Individuals commit occupational fraud costing businesses considerable sums of money, worldwide a potential global fraud loss of more than $3.5 trillion, according to the ACFE report. The median loss, the report states, was $140,000. More than one-fifth of the frauds involved losses of at least $1 million and the frauds lasted a median of 18 months before being detected. It can be seen that any methodology that can be used to improve fraud risk management must be seriously considered.

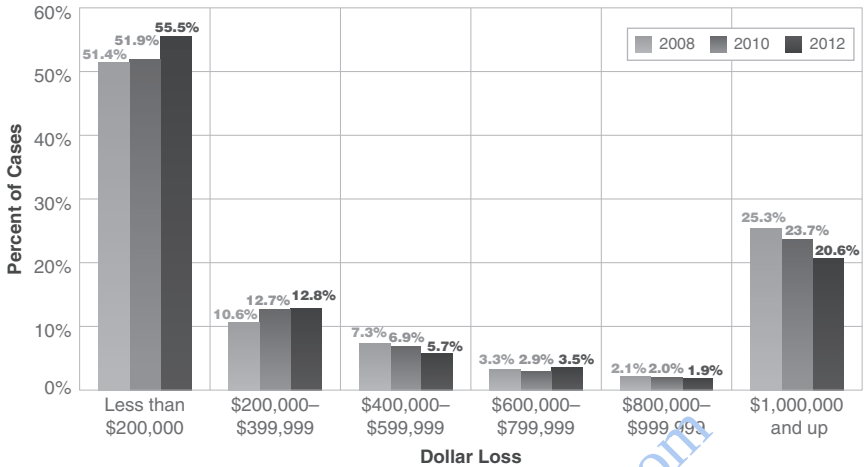

FIGURE 1.1 Distribution of Dollar Losses. *Source:* ACFE, *Report to the Nations*, 2012.

TYPES OF OCCUPATIONAL FRAUD

The top three classifications or means of committing occupational fraud are *corruption*, *asset misappropriation*, and *fraudulent financial statements*, as depicted in Figure 1.2.

Within each classification is a myriad of types and schemes that need to be understood when considering methodology profiling. As indicated in Figure 1.3, asset misappropriation is by far the most frequent form of occupational fraud, comprising 87 percent of the cases reported; it was also the least costly form of fraud, with a median loss of $120,000.

At the lower end of the frequency spectrum are cases involving financial statement fraud. Financial statement fraud was, however, by far the most costly form of occupational fraud. Financial statement fraud schemes made up just 8 percent of the cases in the ACFE study, but caused the greatest median loss, at $1 million. Corruption schemes fell in the middle, occurring in just over one-third of reported cases and causing a median loss of $250,000, with asset misappropriation having the lowest median loss, as depicted in Figure 1.4.

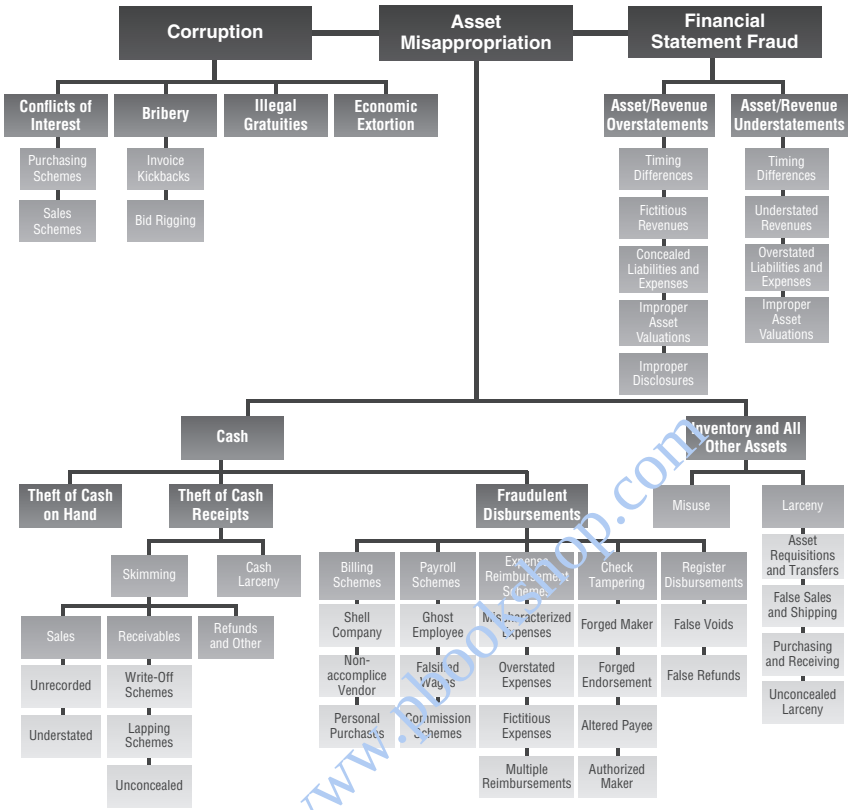

FIGURE 1.2 Classification of Occupational Fraud and Abuse. *Source:* ACFE, *Report to the Nations*, 2012.

High-level or owner/executive perpetrators cause the greatest fraud loss to their organizations, in terms of monetary value rather than quantities of frauds. This is particularly shocking considering that the "tone at the top" is considered to be a fundamental constituent part of a sound antifraud program. In actual fact frauds committed by owners/executives were more than three times as costly as frauds committed by managers and more than nine times as costly as other employee fraud, according to the ACFE. Executive-level fraud also took much longer to detect.

The most common executive-level fraud, according to the survey, is corruption (54 percent of cases), followed by fraudulent invoicing schemes

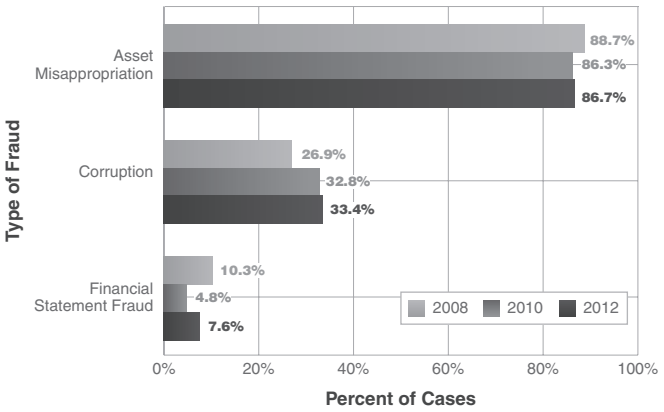

FIGURE 1.3 Occupational Frauds by Category—Frequency. *Source:* ACFE, *Report to the Nations*, 2012.

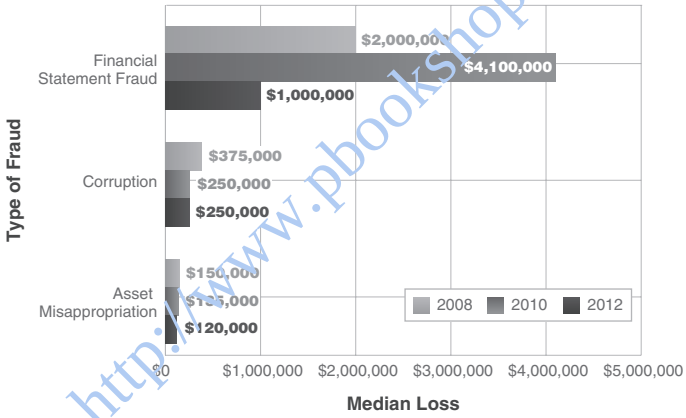

FIGURE 1.4 Occupational Fraud by Category—Median Loss. *Source:* ACFE, *Report to the Nations*, 2012.

(33 percent), expense reimbursement fraud (21 percent), and fraudulent financial statements (21 percent). Other schemes include payroll fraud, check tampering, and cash theft.

EARLY FRAUD

Business has been around for thousands of years, and the way it is run and sometimes abused can be embedded deep in the culture. Occupational fraud

was defined by American criminologist Edwin H. Sutherland (1883–1950) as "a crime that involves a betrayal of trust implied in the holding of an office or other position of trust." Sutherland used the term *white-collar crime*, casting doubt on the idea that poverty breeds crime. Sutherland argued in *White Collar Crime* that members of society occupying positions of privilege and status were just as likely to commit crime as those from lower classes. Sutherland's work, it could be argued, reflects some of the earliest studies on profiling criminals.

It can be contended that rationalization of occupational crime comes from its low visibility, occurring under cover of employment, with victims often suffering without meeting perpetrators, resulting in the indirect nature of the act giving the appearance that it is victimless. Research shows, however, that occupational fraudsters display criminal thinking that parallels street-level offenders with similar behavioral traits that serve as risk factors.

Generally, fraudsters live well-ordered lives and are well respected in their communities and at work. They commit fraud in their workplace to fulfill a financial need when there is an opportunity to do so and when then can rationalize their deed (Cressey's fraud triangle, 1953). Trusted, well-paid employees risk their careers by stealing from their employers due to financial difficulties, lifestyle maintenance, anger, low loyalty, revenge, and boredom (KPMG, 2011). Occupational fraud is costlier than other crimes and affects more people (ACFE, *Report to the Nations*, 2012). It relies on deceit and concealment and often employs sophisticated technology.

Further to motive and opportunity, techniques of neutralization enable individuals to violate normative and ethical standards (Coleman, 2002). For example, by justifying theft as "borrowing," criminal activities may be deemed to be a normal way of stealing or achieving business targets. Trying to prove that a fraudster intends to permanently deprive an organization can be difficult when the fraudster has claimed that he intends to repay the amount or has already done so. Offenders may justify their behavior by claiming that they are not really hurting anyone, that everyone else is doing it, or that the activities may have been carried out that way for many years. This may be a reflection on their culture or background.

The ACFE estimates that some $3.5 trillion of fraud is happening worldwide. The National Fraud Authority in the United Kingdom publishes its Annual Fraud Indicator every year, which estimates that fraud in 2011 was costing the UK economy over £38 billion a year, equating to a shocking £765 per adult per year. This figure includes estimated undetected losses.

In the *Compliance Reporter* article "UK Fraud at Record Level" (2012), KPMG reported the actual 2011 UK fraud to be £3.5 billion. The 2011 *FraudTrack Report*, released by accountancy firm BDO, revealed a significant

increase in both the number and value of reported frauds in the United Kingdom in the previous year to the highest level of fraud since the report began in 2003. In 2010, there were 372 cases of reported fraud with an average value of £3.7 million each. This had risen to 413 cases with an average value of £5 million each.

THE FIGHT AGAINST FRAUD

The nature and threat of occupational fraud is universal, according to the ACFE. Although the research in its 2012 *Report to the Nations* noted some regional differences in the methods used to commit fraud, as well as organizational approaches to preventing and detecting it, many trends and characteristics are similar regardless of where the fraud occurred. Whereas this may make writing a textbook on how to deal with fraud a little easier in that much of the approach may take a standardized approach, this is certainly not the case when we start to consider profiling. Profiling the human being cannot be a standard process with a one-size-fits-all solution. Each human being has unique characteristics and behavioral attributes, thereby giving a unique angle to what may be described as universal fraud.

Providing individuals with a means to report suspicious activity is a critical part of any antifraud program. Fraud reporting mechanisms, such as communication channels and whistleblowing hotlines, should be set up to receive tips from both internal and external sources and should ideally be externally managed, should offer anonymity and toll-free calling, and should allow confidentiality. Management should actively encourage employees to report suspicious activity, offering a reporting process free of reprisals and with the maximum protection for the whistleblower. In many jurisdictions this protection comes through the legal system with whistleblower protection embedded in local law. Interestingly, where I have worked on introducing whistleblowing mechanisms in organizations in jurisdictions where there is no legal protection for whistleblowers, I strongly advise that the organization's CEO or chairman state in his launch address as well as in his preamble in the whistleblowing policy that he personally guarantees the protection of whistleblowers and that their actions will not be detrimental to them in any way, irrespective of legal protection or its absence.

External audits should not be relied on as an organization's primary fraud detection method, says the ACFE. Such audits were the most commonly implemented control in the study; however, they detected only 3 percent of the

frauds reported and they ranked poorly in limiting fraud losses. While external audits serve an important purpose and can have a strong preventive effect on potential fraud, their usefulness as a means of uncovering fraud is limited. Both internal and external auditors, however, have access to and are therefore crucial to the collection and analysis of the information and data required to set up a profiling mechanism in the organization.

Targeted fraud awareness and sensitization training for employees and managers is a critical component of an effective antifraud program and is a proven method of preventing and detecting fraud. Not only are employee tips the most common way occupational fraud is detected, but the research shows that organizations that have antifraud training programs for employees, managers, and executives experience lower losses and shorter fraud durations than organizations that do not have such programs in place. At a minimum, staff members should be sensitized as to what fraud actually is, what actions constitute fraud, how fraud harms everyone in the organization, and how to report suspected fraudulent activity.

Research continues to show that small businesses are particularly vulnerable to fraud. These organizations typically have fewer resources than their larger counterparts, which often translates to fewer and less-effective antifraud controls. In addition, because smaller businesses have fewer resources, the losses they experience tend to have a greater impact than they would in larger organizations. Managers and owners of small businesses should focus their antifraud efforts on the most cost-effective control mechanisms, such as hotlines, employee training and setting a proper ethical tone at the top and within the organization. Additionally, assessing the specific fraud schemes that pose the greatest threat to the business can help identify those areas that merit additional investment in targeted antifraud controls. The fraud risk assessment process is invaluable in determining fraud risk exposure and is a fundamental element of fraud profiling.

PROFILING AS A SOLUTION

In terms of profiling, most fraudsters exhibit behavioral traits that can serve as warning signs of their actions. These red flags, such as living beyond one's means or exhibiting excessive territorial control issues, generally will not be identified by traditional internal controls that are designed to focus on the organization's processes rather than human behavior. Managers, employees, and auditors should be educated through the training and sensitization programs

on these common behavioral patterns and encouraged to consider them, particularly when noted in tandem with other anomalies, to help identify patterns that might indicate fraudulent activity.

The cost of occupational fraud, both financially and, possibly more important, to an organization's reputation, can be acutely damaging. With nearly half of victim organizations unable to recover their losses, proactive measures to prevent fraud are critical. Management should continually assess the organization's specific fraud risks and evaluate its fraud prevention programs in light of those risks. Profiling of the fraudster and his modus operandi will be a valuable addition to the fraud fighter's toolkit.

The fact that the level of reported fraud is up is worrying, but not at all surprising. When the economic climate is difficult there is even more focus on the bottom line and driving out unnecessary costs, so fraud is more likely to be uncovered. Companies should have a proactive approach to fraud protection to avoid increases in the level of fraud. Organizations need to be taking a profit-and-loss approach to fraud risk. If companies continue to take a reactive approach to preventing fraud, it will continue to rise year after year. You cannot design all fraud risk out of a business, but you can put tripwires in place.