CHAPTER ONE

Introduction

ORGANIZATIONS GENERATE AND RETAIN more information stored in electronic format than ever before, yet even though there is more analysis performed with the available data, fraud persists. With such vast amounts of data, abusive scheme transactions are hidden and are difficult to detect by traditional means. Data analytics can assist in uncovering signs of potential fraud with the aid of software to sort through large amounts of data to highlight anomalies.

This book will help you understand fraud and the different types of occupational fraud schemes. Specific data analytical tests are demonstrated along with suggested tests on how to uncover these frauds through the use of data analytics.

DEFINING FRAUD

A short definition of fraud is outlined in *Black's Law Dictionary*:

> An act of intentional deception or dishonesty perpetrated by one or more individuals, generally for financial gain.[1]

This simple definition mandates a number of elements that must be addressed in order to prove fraud:

- The statement must be false and material.
- The individual must know that the statement is untrue.
- The intent to deceive the victim.
- The victim relied on the statement.
- The victim is injured financially or otherwise.

The false statement must substantially impact the victim's decision to proceed with the transaction and that perpetrator must know the statement is false. A simple error or mistake is not fraudulent when it is not made to mislead the victim. The victim reasonably relied on the statement that caused injury to the victim or placed him or her at a disadvantage.

It is intentional deception that induces the victim to take a course of action that results in a loss that distinguishes the theft act.

In addition to the employer suffering a financial or other loss, occupational fraud involves an employee violating the trust associated with the job and hiding the fraud. The employee takes action to conceal the fraud and hopes it will not be discovered at all or until it is too late.

The word *abuse* is employed when the elements for defining fraud do not explicitly exist. In terms of occupational abuse, common examples include actions of employees:

- Accessing Internet sites such as Facebook and eBay for personal reasons.
- Taking a sick day when not sick.
- Making personal phone calls.
- Deliberately underperforming.
- Taking office supplies for personal use.
- Not earning the day's pay while working offsite or telecommuting.

There is an endless list that can fall under the term *abuse*, but no reasonable employer would use this word to describe any employee unless the actions were excessive. Organizations may have policies in place for some of these items, such as an Acceptable Internet Use Policy, but most would be considered on a case-by-case basis, as the issue is a matter of degree that can be highly subjective. There would unlikely be any legal actions taken against an employee who participated in a mild form of abuse.

ANOMALIES VERSUS FRAUD

In the data analysis process, "Detecting a fraud is like finding the proverbial needle in the haystack."[2] Typically, fraudulent transactions in electronic records are few in relation to the large amount of records in data sets. Fraudulent transactions are not the norm. Other anomalies, such as accounting records anomalies, are due to inadequate procedures or other internal control weaknesses. These weaknesses would be repetitive and will occur frequently in the data set. Sometimes, they would regularly and consistently happen at specific intervals, such as at month- or year-end. Understanding the business and its practices and procedures helps to explain most anomalies.

TYPES OF FRAUD

The Association of Certified Fraud Examiners (ACFE) in the 2012 Report to the Nations[3] outlines the three categories of occupational fraud and their subcategories in Figure 1.1.

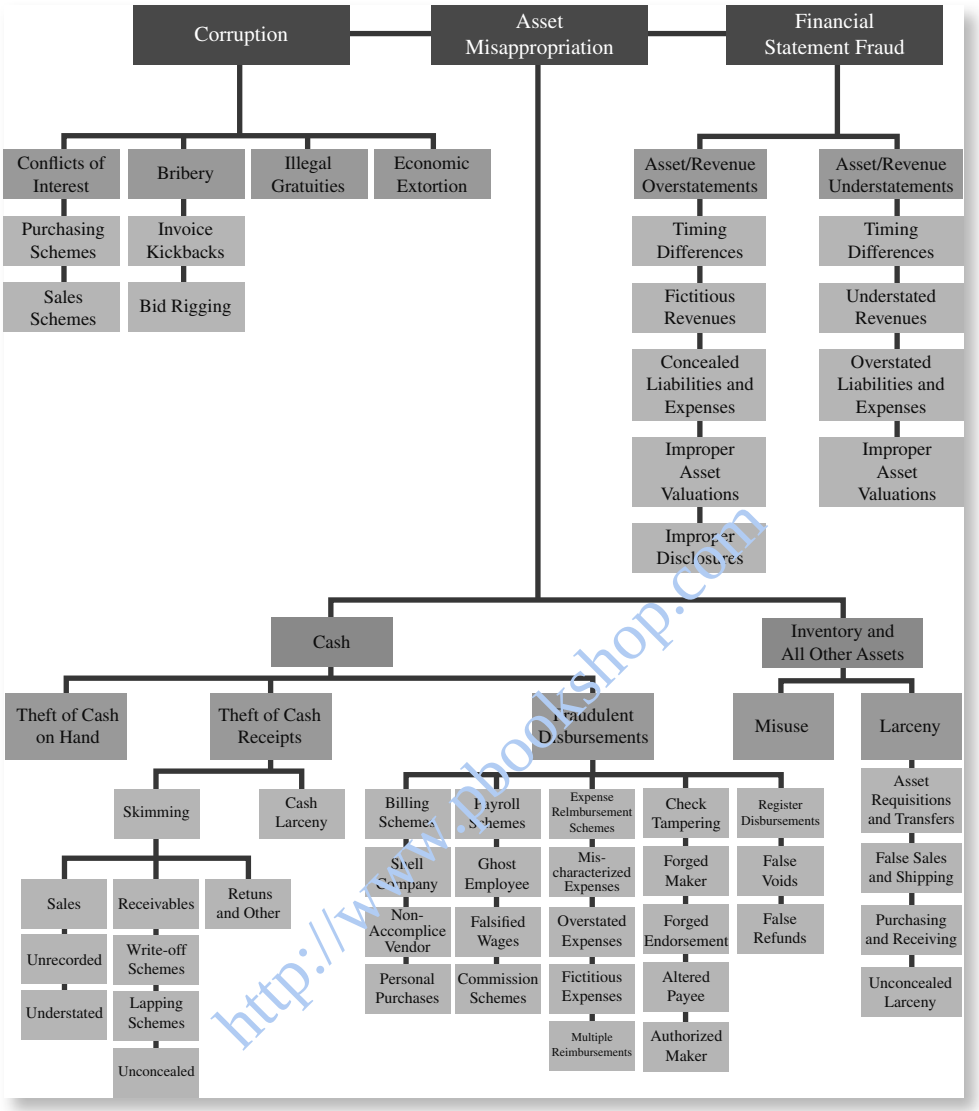

FIGURE 1.1 Occupational Fraud and Abuse Classification System

Source: Association of Certified Fraud Examiners

It was found that:

As in our previous studies, asset misappropriation schemes were by far the most common type of occupational fraud, comprising 87% of the cases reported to us; they were also the least costly form of fraud, with a median loss of $120,000. Financial statement fraud schemes made up just 8% of the cases in our 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.[4]

Among the three major categories—corruption, asset misappropriation, and financial statement fraud—there are far more types of occupational fraud in the asset-misappropriation category. There are many known schemes and areas where fraud may occur. Thefts of cash on hand have been occurring ever since there was cash. With globalization and the availability of the Internet, newer and more innovative types of fraud are coming to light.

An example is the case study published in Verizon's security blog titled "Pro-Active Log Review Might Be a Good Idea."[5] A U.S .-based corporation had requested Verizon to assist them in reviewing virtual private network logs that showed an employee logging in from China while he was sitting at his desk in the United States. Investigation revealed that the employee had outsourced his job to a Chinese consulting firm at a fraction of his earnings. The employee spent most of his day on personal matters on the Internet. The blog notes that the employee's performance reviews showed that "he received excellent remarks. His code was clean, well written, and submitted in a timely fashion. Quarter after quarter, his performance review noted him as the best developer in the building."

Clearly there was no dispute with the quality of work submitted and he had met all deadlines. While the employee did misrepresent that the work was his, the company did not suffer any direct financial loss. Other than violating security policy of permitting unauthorized access to the network, at most, the employee abused company resources by browsing the Internet for most of his workday.

Would any of this have been an issue if the employee were a contractor who subcontracted his work out (assuming that there were no objections with the login procedures)?

ASSESS THE RISK OF FRAUD

It is not possible to eliminate fraud risk in any given area other than to avoid it all together. A company may choose not to deal with a particular vendor or purchaser. They may choose not to acquire assets that need a high level of protection or to expand or do business in an unstable country. Alternatively, they may select an exit strategy if the risk is found to be too great. Avoidance would have been the result of either a formal or informal risk assessment. A risk analysis would have been considered and found that the cost outweighs the benefits.

Some risks will be assumed without additional control features being implemented, since the cost of implementation would be higher than the expected loss. For example, banks issuing credit cards may be able to reduce fraudulent charges if they implement new high-tech security measures, but the cost in terms of dollars or customer inconvenience would be higher than the cost of fraudulent transactions. Fraud is a cost of doing business and it needs a cost-to-benefit or return-on-investment analysis. The risk assessment aids in the determination of the level of controls to implement while balancing acceptable risk tolerance against costs of reducing the risk.

$$\text{Risk} = \text{Impact} \times \text{Probability (threats and vulnerabilities)}$$

In most cases, the company will seek to mitigate the risks by implementing controls. These could be preventative, monitoring, or detection controls. Risk can also be mitigated by purchasing insurance or, in the case of certain employees, requiring them to be bonded.

It may be determined that costs exceed the benefits of preventing fraud in a particular area. However, investments in measures to detect rather than prevent the fraud may be an acceptable risk given the lower costs and likelihood of high losses. Detective measures must also be factored into any risk assessment.

The decision on how far to go will depend on the risk assessment and the reason for performing the risk assessment. It is a management decision as to what level to take the response to the risk of fraud. The decision will be primarily based on why the fraud risk assessment was undertaken in the first place. Was it due to audit or regulatory requirements? Was it management's desire to evaluate the internal control system? Was it to reduce the cost for fraud?

A risk assessment will identify potential areas of fraud, whether internal or external, directly or indirectly, and how vulnerable or how likely the threat is to occur. Factors that determine the probability component include:

- The industry or nature of the business
- The values and ethics of senior management and employees
- Internal controls—preventive and detective
- Business environment—local versus multinational, small versus large, brick-and-mortar versus Internet, geographic location, economic conditions
- Likelihood
- Industry trends
- History
- Resources
- Internal control
- Complexity
- Volume
- Standards
- Whistleblower
- Complaints
- Moral
- Impact
- Value
- Maximum exposure

Other issues that must be considered when performing a risk assessment include the possibility of adverse publicity resulting in a loss of consumer confidence, potential lawsuits, violating laws, and the overall impairment to carrying on normal business.

Appendix D of *Managing the Business Risk of Fraud*[6] is an excellent example of the fraud-risk assessment framework for revenue recognition risk that can be used as a template for any organization. It can also be modified to encompass any type of risk.

The template lists various fraud risks and schemes and then associates the following with each of the schemes:

- Likelihood of occurrence
- Significance to the organization

- People and/or department subject to the risk
- Existing antifraud internal controls
- Assessment of internal control effectiveness
- Residual risks
- Fraud-risk response

CONCLUSION

Understanding what fraud is and the types of frauds allows us to focus on occupational fraud in this book. Being able to assess fraud risk provides us with priorities as to where to invest time and resources to have the largest impact in detecting and reducing incidents of fraud.

NOTES

1. *Black's Law Dictionary*, "What Is FRAUD?," accessed June 17, 2013, http://thelawdictionary.org/fraud-2.
2. Steve W. Albrecht et al., *Fraud Examination*, 4th ed. (Mason, OH: Cengage Learning, 2012).
3. "Association of Certified Fraud Examiners—2012 Report to the Nations," accessed June 17, 2013, www.acfe.com/rttn.aspx.
4. Ibid.
5. Andrew Valentine, "Case Study: Pro-Active Log Review Might Be a Good Idea," Verizon Enterprise Solutions, accessed April 24, 2014, www.verizonenterprise.com/security/blog/index.xml?postid=1626.
6. Institute of Internal Auditors, the American Institute of Certified Public Accountants, and Association of Certified Fraud Examiners, *Managing the Business Risk of Fraud: A Practical Guide*, https://na.theiia.org/standards-guidance/Public%20Documents/fraud%20paper.pdf.