

# RISK INSIGHTS



weaver  risk advisory services

## STOP FRAUD IN ITS TRACKS } *Don't wait until you are working on fraud detection in your company*

### *What happens when fraud is detected in an organization?*

The most direct cost of that fraud may be measured by the amount of assets stolen, or in the difference between actual financial performance and what was presented in misstated reports. Costs may extend to stockholders, current and retired employees, vendors, customers and others.

Business disruption accompanies fraud investigations, as do possible lawsuits and criminal charges. Although more difficult to quantify, the long-term losses of confidence and trust among all stakeholders may be the highest costs organizations face when exposing fraud. Recovering from those losses can take years, and sometimes the damage is so severe that recovery is not possible.

The financial costs alone are staggering:

- ***\$2.9 trillion lost annually to fraud by entities throughout the world and their various stakeholders.***
- ***\$160,000 lost in the median Asset Misappropriation scheme.***
- ***\$250,000 median loss in Corruption schemes.***
- ***\$1 million or more lost in almost 25 percent of investigated fraud cases.***
- ***\$4 million lost in the median Financial Statement Fraud case.***
- ***\$155,000 median loss in fraud schemes involving an organization with 100 employees or less.***

Those damage assessments are derived from the most recent 2010 edition of the Association of Certified Fraud Examiners (ACFE) Report to the Nations on Occupational Fraud and Abuse. The ACFE, an international

society of fraud investigation professionals, evaluated findings from 1,843 fraud investigations conducted throughout the world by its members between January 2008 and December 2009. Perhaps the study's most unsettling finding is this:

- ***The typical organization loses 5 percent of its annual revenues to fraud.***

Fraud is that destructive and that pervasive; it does not just happen to other people or other organizations. A typical fraud scheme goes undetected for two years 18 months. When fraud is discovered, the full amount of the known tangible losses is seldom recovered. Recovering the intangible assets that fraud takes – assets such as corporate goodwill, credibility and trust – is even more difficult.

Making every reasonable effort to keep fraud from occurring is less costly and far less daunting than addressing its aftermath. That emphasis on prevention begins with understanding the various ways fraud is executed, and the general principles that deter fraud.

### **The Primary Categories of Fraud**

Fraud affects so many entities and it manifests itself in an array of schemes. Those schemes are usually encompassed within the following three major categories of occupational fraud and abuse:

- ***Asset Misappropriation***
- ***Corruption***
- ***Financial Statement Fraud***

Asset Misappropriation is the most common and inclusive form of occupational fraud, striking large and small entities within the public, private, and nonprofit sectors. Asset misappropriation includes incidents of fraudulent invoicing, payroll fraud, larceny, and revenue skimming. While such schemes usually center on cash, they also include thefts of raw materials, supplies, merchandize and other inventory.

**“FINANCIAL STATEMENT FRAUD  
COMPRISES THE THIRD MAJOR  
CATEGORY OF OCCUPATIONAL FRAUD.”**

Corruption defines instances where an individual seeks to benefit in a manner contrary to that person’s fiduciary responsibilities and duties to his or her employer. Corruption schemes include awarding business to a vendor in exchange for kickback payments, offering or accepting bribes, or failing to disclose a conflict of interest that could influence business decisions and related transactions. Corruption occurs less frequently than Asset Misappropriation, but the median cost per scheme is much higher.

Financial Statement Fraud comprises the third major category of occupational fraud and abuse. It includes various ways financial statements are falsified to provide an inaccurate view of company performance. Those schemes included classifying revenue-based expenses as capital expenditures to hide losses and increase net income, not recognizing expenses in the proper reporting period, or recording pending sales as completed transactions. In some cases, sales revenues are totally fabricated.

The median loss per financial statement fraud case of \$4 million makes financial statement fraud the costliest fraud category, even though such cases comprise a small fraction of total fraud investigations.

### **Fraud Threatens an Organization’s Existence**

Estimated losses topped \$1 million in hundreds of fraud schemes this past decade. With too many billion-dollar losses occurring, the investing public have lost confidence in the public market.

Billion-dollar fraud cases involve very large entities. Due to disclosure requirements and ensuing media coverage, such situations capture considerable public attention. However, smaller businesses suffer a greater adverse impact from fraud but this most often goes unnoticed.

The median loss suffered by an organization with less than 100 employees is \$155,000 per fraudulent scheme. Per employee, fraud strikes small businesses much harder than it hits this nation’s largest corporations.

Smaller organizations often do not establish and maintain necessary preventative and detective controls, and rely instead upon trust. Too often, individuals have too many responsibilities, with too little oversight. Smaller companies often do not run background checks on potential employees, making them more vulnerable toward hiring individuals who

have committed fraud and workplace theft elsewhere. However, unsolicited business references that are generated based on employment history is also advisable as many fraud cases go unreported and unprosecuted. The most common schemes affecting smaller businesses include writing fraudulent checks, skimming revenues, and processing fraudulent invoices.

The damage caused by fraud cannot be measured strictly in documented financial losses, either. Profound, personal feelings of betrayal accompany fraud revelations. Investigations and ensuing litigation cause prolonged business disruption. Bankers, customers, employees, investors, vendors and others lose trust and confidence in the organization. Recovering from such damage can take years, and sometimes the impact is so severe that recovery just is not possible.

### **Elements of Effective Fraud Prevention**

Fraud prevention helps keep organizations from ever having to confront such consequences. An emphasis on prevention begins with recognizing that perceived opportunity is a common driver behind so many fraudulent schemes.

When proving that fraud has occurred, the five elements to focus on are intent, motive, opportunity, repetitive acts and concealment. Even in the instances where intent and motive are present, specific controls should be developed to prevent opportunity, repetitive acts and concealment from occurring. Opportunity is the one element that organizations have the most controls over.

Individuals have differing motives for considering fraudulent behavior. Some may want to live lifestyles they cannot otherwise afford. Some may be seeking ways to resolve personal financial difficulties. Some may feel resentment toward their employers and may rationalize that committing fraud is just a form of payback. Others may be seeking acclaim from various stakeholders that has not been earned by actual performance.

Whatever the underlying motivations or rationalizations may be, perceived opportunity – a person’s belief that he or she can execute fraud without getting caught – is a crucial factor in whether an individual acts upon an improper impulse or motive. A fundamental principle of effective fraud



Such technological capabilities enable organizations to analyze, generate, transmit and store immense volumes of data much more efficiently. Those same capabilities, however, also expose organizations to fraudulent activities initiated with keystrokes and mouse clicks.

prevention is removing that perception of opportunity.

Management sets the “tone at the top” by emphasizing and continually communicating the importance of honest, ethical behavior. Investigation of tips regarding suspected improper activity is the most commonly-cited means for detecting fraud. By regularly emphasizing fraud prevention, management creates an internal culture where individuals feel comfortable and compelled to report possible fraud, either through an anonymous 24-hour hotline, or in person. Such a culture dispels perceptions of opportunity.

Incorporating the concept of segregation of duties into individual job descriptions and responsibilities further combats that perception of opportunity and establishes boundaries that prevent fraudulent activity from occurring. Segregation of duty is a foundational element of preventative fraud controls.

Segregation of duties separates incompatible responsibilities that present inherent conflicts of interest. That segregation establishes a natural system that of checks and balances that not only deters fraud but also reduces errors. Incorporating segregation of duties, for example, means not having the same person being responsible for ordering materials and ensuring that those shipments arrive as ordered.

That segregation of duties needs to be reflected in computer access controls, too. Such practices ensure, for example, that an individual cannot have access to all of the applications, files and functions needed to execute a fraudulent transaction.

In addition to maintaining segregation of duties within IT access privileges, managers also need to recognize the advantages and fraud risks that accompany reliance upon IT in general. Several decades ago, companies needed large warehouses to hold processed claims, health care records, sales receipts, purchase orders, invoices, and other crucial forms of documentation. Such files today typically reside in a data warehouse or other electronic storage repository, greatly reducing the need for physical security measures.

Such technological capabilities enable organizations to analyze, generate, transmit and store immense volumes of data much more efficiently. Those same capabilities, however, also expose organizations to fraudulent activities initiated with keystrokes and mouse clicks. In addition to money, individuals often target nonpublic information that can be used in identity theft schemes. IT operability and security issues, such as data integrity, file protection, network safety, and authorized change management practices are now fraud prevention issues, too.

Implementing and sustaining fraud prevention measures incurs initial costs and continual expense. The total expense, however, is typically less than the cost associated with just one incident of fraud detection.

Due to the complex steps individuals take to hide evidence of fraudulent activity, calculating the exact financial losses suffered in such cases is difficult. Fraud prevention functions as a form of insurance, an insurance that saves organizations from having to make all of the costly and difficult calculations that accompany fraud detection.

## SPOTLIGHT

**Alyssa G. Martin, CPA, MBA**, is the Partner-in-Charge of Advisory Services at Weaver. Weaver is ranked the largest independent certified public accounting firm in the Southwest by Accounting Today. Martin can be contacted at 817.332.7905 or 972.448.6975. You may learn more about Weaver by visiting [www.weaverllp.com](http://www.weaverllp.com).

## CONTACT US

**ALYSSA G. MARTIN, CPA, MBA**  
*Partner, Advisory Services*

[alyssa.martin@weaverllp.com](mailto:alyssa.martin@weaverllp.com)  
817.332.7905 or 972.448.6975

Weaver has offices throughout Texas.  
More at [weaverllp.com](http://weaverllp.com)



# STAY IN CONTROL.

Today, objectivity is essential in identifying and managing risks. Focus, strategy and communication create the foundation for assessments that are well-planned, executable and measurable. At Weaver, our goal is to help you improve your financial accounting and reporting in the industry. We work closely with you to model services to fit your organization's existing structure, process and staffing.

Our team is backed by the technical and industry-specific knowledge of our professionals. Weaver's internal control approach focuses not only on regulating risks, but also on enhancing operational efficiencies. And with our Advisory Team, you get responses that are prompt, accountable and goal focused.



2821 W. 7<sup>TH</sup> STREET, SUITE 700, FORT WORTH, TX 76107

WEAVER AND TIDWELL LLP  
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS  
[WWW.WEAVERLLP.COM](http://WWW.WEAVERLLP.COM)

Presorted Standard  
U.S. Postage  
PA I D  
Fort Worth, Texas  
Permit # 886

This newsletter is general in nature and is not a substitute for accounting, legal or other professional services. We assume no liability for the reader's reliance on this information. Before implementing any of the ideas contained in this publication, consult a professional advisor to determine whether they apply to your unique circumstances.