

# SHOULD YOU BE CONCERNED WITH FRAUD?

By Joseph S. Barbagallo, CAP, CVA, CFFA, Principal

It is generally acknowledged by the business community that fraud is a major problem costing billions of dollars every year. In the post Enron and World Com days, the general public and many investors seem to be concerned with fraud related to large public companies. But should this be the only concern?

According to the "2002 Report to the Nation on Occupational Fraud and Abuse" published by the Association of Certified Fraud Examiners, the average business organization loses in excess of \$9 per day per employee due to fraud. The most costly fraud abuses occurred in companies with less than 100 employees. The average loss per fraud scheme in small businesses was actually higher than the average loss in the largest companies. According to a survey in a global report by PriceWaterhouseCoopers, thirty seven percent of respondents reported significant economic crimes during the two previous years. It is obvious then, that nearly all businesses need to be concerned with fraud.

Let's look at the three major categories of fraud, who commits fraud, and what can be done to reduce the risk of fraud.

## **THREE CATEGORIES OF FRAUD**

The three major categories of fraud are financial reporting fraud, misappropriation of assets, and external fraud.

Financial reporting frauds are the intentional misstatement of either amounts, disclosures, or both in financial statements. This type of fraud, also known as management fraud, is done to mislead those relying on the financial statements to achieve an outcome related to things such as a bonus, financing, a company's valuation, etc.

Misappropriation of assets, commonly referred to as employee fraud, is the theft of an organization's assets by employees. Some of the most common types of misappropriation of assets are the following:

1. The theft of cash by skimming or diverting cash receipts, manipulation of accounts receivable postings (lapping), stealing or forging checks, stealing petty cash, altering bank deposits, or phony refund schemes.
2. Creating fictitious vendors or overstating vendor invoices.
3. Taking kickbacks
4. The theft of equipment or inventory
5. Abusing travel and entertainment

6. Payroll schemes such as adding ghost employees or overpaying wages or commissions. At times, the employee may find it necessary to manipulate financial records to conceal their misappropriation of assets but this is considered secondary to the primary purpose of the theft or assets. In the theft of assets, cash is targeted 90% of the time.

The third category of fraud, external fraud, is generally committed against the organization by people outside the organization (non-employees). Examples of external fraud are altering and cashing a check or delivering sub-standard materials to a construction site. In some cases a person outside the organization may collude with an employee.

## **WHO COMMITS FRAUD**

Numerous research projects have been performed to determine why a person commits fraud. Research from various fields and disciplines has identified what determines whether an individual will commit fraud. The three factors, referred to as the “fraud triangle”, are motive or perceived pressure facing the individual, opportunity to commit fraud, and rationalization or lack of integrity. The fraud triangle can be easily remembered by the fraud perpetrators wanting “M O R (E)” (i.e. motive, opportunity and rationalization). The following is a brief discussion of each factor:

Motive - Pressures that motivate a person to commit fraud may be financial or work related. Financial pressures could develop from things such as a drug, alcohol or gambling habit or an extramarital affair. Work related factors include things such as not being promoted, feeling overworked or under paid which prompt a person committing fraud to get even.

Opportunity - Opportunities to commit fraud can arise when internal controls are weak or non existent or when an employee is trusted too much. Perpetrators are limited to opportunities which are available to them but the opportunities can be expanded by collusion. Even when good controls exist, a person with trust or authority may be able to override the controls or direct subordinates to skip a control procedure. Some examples of conditions which provide opportunity for a person to commit fraud are lack of segregation of duties, absence of mandatory vacations, failure to inform employees about company policies and procedures (or lack of enforcing them), rapid turnover of employees or constant operation under crises.

Rationalization - Many different rationalizations can be typical from a person committing fraud. Some examples of rationalizations are “I was treated unfairly and the company owes me,” “It won’t hurt anyone,” “I am using the money for a good cause,” “I will pay it back later,” and numerous others.

This third factor in this fraud triangle is generally considered the most important. Many people who have pressure or opportunity to commit fraud do not due to personal integrity.

In order to reduce the risk of fraud, an organization should implement policies and procedures which respond to the three elements on the fraud triangle. The three methods to address the elements of the fraud triangle are creating an ethical environment, reducing the opportunity to commit fraud and monitoring and developing appropriate responses to pressure on employees to commit fraud.

## **WHAT CAN BE DONE TO REDUCE THE RISK OF FRAUD**

To create an ethical environment an employer should investigate new hires and employees, perform drug testing, have integrity testing, implement an ethics policy (preferably with signed ethics statements), bond employees and prosecute fraud perpetrators.

Employers should monitor pressure on employees and develop appropriate responses by performing drug testing, instituting appropriate personnel policies and procedures, and providing counseling services.

There are many controls a business can institute to reduce an employee's opportunity to commit fraud by preventing fraud from occurring or detecting fraud in a timely manner before it has occurred. Examples of procedures which could reduce opportunity are hiring spotters or instituting surveillance techniques, job rotation and mandatory vacation policies, preparing timely financial statements for review, and implementing an employee hotline.

One of the most effective and important deterrents to fraud is a strong system of internal control. Strong controls can deter fraud or allow for early detection. Weaknesses in internal control may not only allow for fraud opportunity but will also allow fraud to go undetected. Designing a system of internal control to prevent misappropriation of assets involves reviewing the components, systems and procedures of internal control within the business as well as identifying assets susceptible to misappropriation and developing controls to reduce the risk of misappropriation.

In developing a system of internal control businesses should consider the cost/benefit relationship of controls. It is almost impossible to design a system of internal control to completely eliminate the possibility of fraud and even if it were possible to design such a system, the cost may be prohibitive. In some case, it may be more effective to design a system to detect and correct errors or fraud in a timely manner after they have occurred.

It should be apparent that any business must be aware of the potential for fraud in the organization and should take a proactive approach to identifying and improving the control structure. A properly designed internal control system will not only help to prevent fraud but will also improve the operational efficiency of a business.