

The Metropolitan Corporate Counsel

Volume 11, No. 1

© 2003 The Metropolitan Corporate Counsel, Inc.

January 2003

Not All Accounting Scandals Make Headlines Beware Of Employee Frauds

By Kyle Anne Midkiff, CPA, CFE

For the past year the news has been overrun by accounts of large accounting scandals, corporate corruption and shareholder frauds. Companies like Adelphia, Enron, Global Crossing, Tyco, and World-Com, previously known only to the investment community, are now household names, which have become synonymous with corporate greed. As a result of these major scandals, on July 30, 2002, President Bush signed the Sarbanes-Oxley Act of 2002 (the Act), the most far-reaching legislation regulating public accounting firms and public companies in decades. Recently much has been written and discussed about the Act and how it will affect the corporate governance and public disclosures of public companies as well as the oversight and conduct of accounting and auditing services.

Given the news hype and regulatory focus on these corporate wide scandals, it is likely that corporate officers and managers have been spending a great deal of time addressing shareholder and regulatory concerns. While some of this attention may be warranted, you cannot ignore the plain vanilla, garden-variety internal frauds and embezzlements that occur on a daily basis and continue to proliferate. These internal frauds and embezzlements occur in all types of entities - including public companies, privately held companies, non-profit entities, and civic associations.

The Association of Certified Fraud

Kyle Anne Midkiff is a Principal in Nihill & Riedley, PC, a forensic accounting firm in Philadelphia, PA. She can be reached at 215-238-8450 or via e-mail at kmidkiff@nihillriedley.com.



Kyle Anne Midkiff

Examiners (ACFE) in their 2002 Report to the Nation, estimated that occupational fraud and abuse will bilk American companies out of \$600 billion this year - the equivalent of \$4,500 per employee. The reasons for the boom in fraud and embezzlement are many, including the usual, such as employees or officers with the right combination of greed, motive, and opportunity. The motives for financial fraud include the intent to increase stock prices, earn fat bonuses, comply with loan covenants, cover up asset misappropriations and fund personal expenses. These characteristics and motives are coupled with environmental factors such as: downsizing of corporations, resulting in reduced internal controls and decreased employee loyalty; headline-grabbing financial scandals which tend to focus a company's attention elsewhere and

cause bitterness and resentment in lower level employees (e.g. "look at what they get away with, I deserve some too"); employee losses in the stock market; and the slow economy.

The old favorite frauds are still the most successful: creating fictitious creditors, payroll ghosts, phantom vendors, skimming cash sales and padding expenses. Sophisticated computer systems have not eliminated fraud - instead they bring new opportunities and methods to the fraudster.

Common Fraud Schemes

Here are examples of the more common fraud schemes to keep in mind to prevent fraud in your company.

Serial Embezzlement

A recent phenomenon is that of the serial embezzler who goes from job to job stealing from each one. In some cases, the serial embezzler steals from the second employer to pay restitution to the first employer. This means, of course, that employer number 2 did not perform adequate due diligence in hiring, and/or that employer number 1 probably kept the embezzlement quiet in order to avoid embarrassment and distasteful publicity.

In other situations, the serial embezzler steals from employer number 1 and moves on to another job when they begin to feel nervous about getting caught. The serial embezzler then continues to steal from each subsequent employer and moves on when there is a fear of discovery. The employers who hire serial embezzlers tend to have certain things in common. First, they did not perform adequate background checks including credit checks on personnel, and second, they trusted the embezzler and gave

Nihill & Riedley, PC (215) 238-8450

them a significant amount of responsibility. Serial embezzlers tend to have certain characteristics in common that should raise red flags for employers. First, they willingly take on responsibility and gladly handle all the details. The more details the embezzler handles, the more theft and cover-up opportunities are provided. Second, the embezzlers suffer from selective messiness that causes missing documents, continued adjustments and confusion which helps mask the theft. These serial embezzlers also have the uncanny ability to identify and hone in on trusting employers and internal control weaknesses that can be exploited.

Revenue Recognition Fraud

The term revenue recognition fraud makes one think of the large frauds against shareholders. However, there are also revenue recognition frauds that occur on a much smaller scale. These frauds occur inside the company, and are usually committed for job security, often in response to pressure from management to achieve earnings targets. For example, in a division of a publicly traded company, management created an environment in which achieving budgeted earnings was of paramount importance and needed to be accomplished at any cost. Of course, there was bonus money at stake if the financial goals were not met. Therefore, to accomplish the unrealistic goals placed upon them by management, required write-offs were delayed and the books and records were kept open for an extra few days to allow for additional revenue to be recognized within the budget period. What were these people thinking? These kinds of revenue recognition schemes eventually catch up with an entity - and the entity is short available revenue to be recorded for the subsequent period. As a result of the improper revenue recognition that occurred, a SEC investigation was launched, several employees were terminated, the company lost money due to the lost productivity, large professional fees were incurred (accountants and lawyers) and a fine was paid to the SEC. This was all to squeeze in a few more dollars of revenue in order to make budget.

This type of fraud also demonstrates that not all frauds are perpetrated for the purpose of taking cash.

Collusion

Another concern is collusion, which makes a fraud more difficult to detect and prevent. Collusion overrides and overcomes the safeguards created to set up strong internal controls, particularly in the area of segregation of duties. Collusion typically occurs over many years and usually involves employees in the accounting

department. A typical example of a scheme that was aided by collusion was a fraud that involved creation of false accounts payable vouchers, falsification of accounts payable checks, misuse of check signing equipment, forgery, recording false expenses in the general ledger, and removing the forged checks when they were returned with the bank statements. Additional side frauds included theft of petty cash, and creation of phantom vendors in the accounts payable system. This fraud totaled in the millions of dollars and endured despite the closing of various bank accounts, the switching of general ledger packages and accounts payable systems several times, and the locking up of the check-signing machine.

Preventing And Detecting Fraud In Your Company

Danger Signs

An entity needs to be aware of the danger signs that may indicate there is increased risk of fraud and that employees are up to something. The following are danger signs that cannot be ignored.

- **Low Morale:** This can result in cutting of corners in the control area.
- **High Staff Turnover:** This can be an indication that employees are distressed with fraudulent activity and are reluctant to continue to work under such conditions.
- **Domineering Management:** Controls may be overridden and key information withheld. These conditions help to mask or conceal fraud.
- **Employee Refusal to Take Vacations and/or Promotions:** The employee needs to stay in his present position in order to maintain the status quo of his or her scheme. Oftentimes, the extra money being obtained from the fraud on a tax-free basis is much better than taking a position with a significant raise.
- **Overemphasis on Achieving Short-Term Financial Goals:** If management becomes too concerned with achieving short-term financial goals, consideration of internal controls and accurate financial reporting are ignored.
- **Remote Locations:** Fraud occurs where supervision and control is least effective or non-existent. Remote locations need to be regularly monitored and visited.
- **Bounced Entity Checks:** If you believe you have the funds and checks are bouncing, chances are something funny is going on.
- **Unusual Write-offs:** If there are unusual write-offs attributed to bad debt, investigation is necessary. The write-offs could be occurring because an employee is stealing the payments and diverting them to their own accounts as they are received.

- **Things Don't Add Up:** If things aren't getting done and don't make sense, a closer look needs to be taken. If something seems wrong, it probably is. Trust your instincts.

Fraud Alerts

The following fraud alerts cannot be ignored. They should be investigated immediately and extensively.

- **Tips:** Tips can come in the form of telephone messages or anonymous letters. They may be frivolous and without merit, but they need to be explored.
- **Lifestyle indications:** An obvious discrepancy in earnings and lifestyle can be a red flag indicating fraud.
- **Peculiar or Irrational Behavior:** If there is a surprising or unexpected change in behavior of an individual, this could be an indication that they are under severe pressure in connection with the perpetration of a fraud.

Safeguarding and Protecting Assets

In order to adequately safeguard assets, the following are key points to consider:

- **Never trust anyone 100%. Or if you do trust, follow the old Ronald Reagan motto, "Trust, but verify"**
- **Get organized:** A disorganized entity is a breeding ground for fraudsters.
- **Pay attention to details**
 - Know your daily checking account balance
 - Require bank statements be immediately reconciled
 - Scan paid bills to make sure there is no overpayment
 - Spot check inventory on a surprise basis
 - Review the mail when it first arrives, unopened

What To Do If You Have Been Defrauded

Few people or entities admit they have been defrauded. By keeping it secret, you allow the fraudster to continue his/her crimes elsewhere. If you don't make a strong public statement that you have been defrauded, you leave yourself open to further violations by others who realize the fraud went unpunished. If you've been defrauded, you need to prosecute to the fullest extent of the law, even if you think there is nothing left to recover. In order to prevent a similar occurrence, it is critical that you undertake a full investigation to understand the methodology employed by the fraudster, the total amount of the loss, and how it was allowed to occur. If you don't know how the fraudster circumvented your controls, you can easily be defrauded again. Always remember the old adage, "Fool me once shame on you, fool me twice shame on me."