

Repetitive Fraud – Lessons in Prevention

Glenn M. Pomerantz, CPA

I am often asked if there are certain frauds that I see over and over again and why such frauds re-occur. In the world of financial reporting fraud, new and creative ways to “cook the books” appear year after year. Stock option backdating and revenue recognition round-tripping are two of my favorites. However, in the employee dishonesty universe, embezzlements and corruption tend to be more mundane and less variable. This article addresses employee dishonesty losses with an emphasis on the mistakes organizations make that fail to prevent, detect or deter these frauds.

Investigative Due Diligence

Over the past few years I have been disturbed by the frequency of my involvement in cases of investigating fraud committed by employees with a felony record. Instances include felons in positions of trust, such as handling cash and other valuable assets, authorizing significant transactions or maintaining the books and records. Some organizations will knowingly give a prior felon a second chance. This is not a moral judgment on such organizations; instead, it's about knowing who you are hiring, promoting or partnering with. Making such decisions with the complete universe of information is a competitive advantage.

Investigative due diligence (“IDD”), background checks, credit and criminal checks are all terms used to describe the process of obtaining information about the people and organizations you are planning to hire or with whom you plan to conduct business. Many companies forego the process entirely. Others elect to perform credit checks without searching for any potential criminal background and still others look for the least expensive manner in which to comply with their own policies and procedures. All of these omissions can be fatal. Furthermore, appropriate background checks that are not updated when an employee is promoted to a position of trust or when a business relationship is expanded can prove detrimental.

Thorough investigative due diligence on potential employees expected to be in positions of trust should include:

- | | |
|---|--|
| 1) Criminal history, to include all jurisdictions where the individual has recently resided | 6) Media search |
| 2) Credit history | 7) National and state sex offender registries |
| 3) Civil litigation | 8) In the case of individuals with a financial services industry background, searches of financial regulators to include the SEC and FINRA |
| 4) Bankruptcies, liens and judgments | 9) Reference checks of past employment |
| 5) Confirmation of educational and professional credentials | |

Positions of trust include, but may not be limited to: those with custody of valuable assets, persons with supervisory accounting and financial roles, compliance personnel, human resource professionals, employees with access to confidential information, certain IT professionals and senior management. Business partners, suppliers, distributors and customers should also not be overlooked.

It can be difficult to keep people without a criminal history away from the temptations or pressures of employee dishonesty. It is regrettable to entrust your organization's future to those with a soiled past when the tools of discovery are at your fingertips.

Segregation of Duties

Opportunity to commit fraud is one of the factors present in the often referred to “Fraud Triangle.” Opportunity may arise when the employee is provided with the tools to execute a fraud without a reasonable deterrence, prevention or detection mechanism in place. Segregation of duties (“SOD”) is one of the most effective internal controls in combating employee fraud. The concept of SOD is to identify all of the following responsibilities in each business process: a) Custody of Assets, b) Record-Keeping, c) Authorization, d) Reconciliation.

Continued on back

When the organization separates these functions among its employees, it has implemented a strong internal control, which may deter and prevent employee fraud. Recognizing that some of the most devastating employee frauds have been committed via employee collusion, it is no less important to segregate duties as collusive fraud is often more complex and difficult for employees to master, sustain and conceal. SOD applies to all phases of accounting in an organization with special emphasis on computer controls – both general and application oriented. Smaller organizations with fewer employees are often challenged in segregating duties. Nonetheless, these entities should assess their risks from lack of SOD, prioritize those risks and attempt to apply sound SOD principles to the risks that retain the highest exposures after considering compensating controls.¹

The most basic SOD principle is separation of responsibilities for custody of assets and record-keeping. Time and time again, we encounter frauds whereby checks are received by an employee who also has the ability to write-off receivables or post accounting entries. Variances to these schemes include employees who may only have a limited role in either custody of assets or record-keeping. An example is an employee who handles returned merchandise and processes credits to the customer's account. Custody of assets with either reconciliation or authorization responsibility can prove similarly fatal. Receipt of customer remittances and responsibility for preparing bank reconciliations is one example while access to inventory and the ability to authorize inventory write-offs is another. These basic SOD principles are sometimes ignored or overlooked in even the most sophisticated organizations. Fast growing companies, smaller sized companies and not-for-profits have fallen prey to fraud disproportionately due to SOD issues.

Human Error

Despite sound internal controls, including appropriate SOD and exemplary background check protocols, numerous organizations fail to prevent fraud² when caused by simple human error. Examples include an accounts payable clerk systematically failing to match a receiving report to an approved invoice and authorized purchase order or an employee in Treasury failing to verify authenticity of a change in wiring instructions. Employees without a view of the big picture, who generally do not understand why they perform a particular control function, present vulnerabilities to the organization. What appears to be an innocent shortcut to an Accounts Payable clerk may defeat a key internal control in the organization's Procure to Pay function. There are a number of ways to address the risk of human error:

- 1) Regularly test compliance for key internal controls.
- 2) Establish monitoring controls to verify that the underlying internal controls are functioning. Monitoring controls are often referred to as controls over controls and may include independent review of exception reports, analytical review and automated identification of unusual transactions.
- 3) Review training and education programs to ensure that employees understand the significance of internal controls for which they are responsible.
- 4) Establish compensating controls where underlying controls are particularly susceptible to human error.

This author has seen a disturbing lack of attention paid to training and education. Companies often underestimate the importance of educating employees how their role fits into the strategic objectives of the organization. Internal controls help achieve those objectives. An employee who has been trained to understand the significance of his or her role will be more likely to perform critical procedures as designed. Furthermore, organizations should treat training and education as a continuous process. Recognize that changes to the company's strategy, methodologies and tools, competitive environment, products and services and a host of other inputs, may require additional employee training and education pertaining to internal controls. Mergers and acquisitions as well as promotions to positions of trust should be obvious triggers for employee training and education.

Having evaluated the carnage from hundreds of employee dishonesty schemes, I have seen patterns emerge in internal control failures. Strategies to combat these internal control failures should include appropriate investigative due diligence on certain new and existing employees and business partners, effective risk-based SOD and targeted education and training programs.

¹ Compensating controls may include owner or independent review of books and records and or independent analytical review of significant accounts.

² Like employee fraud, fraud committed against the organization by an outside party is often not prevented or detected due to employee error.

