Internal Fraud: A Proactive Stance Reduces the Allure and Risks

Arthur F. Rothberg, Managing Director, CFO Edge, LLC

There are a myriad of ways an employee can steal from an employer. One common practice is to get the organization to issue a payment for a fraudulent purpose. Based on false information, such as an invoice from a non-existent vendor, a forged receipt or an incorrect timecard, the organization makes a payment which the dishonest employee then pockets, spends or banks. The use of company credit cards, debit cards and purchase orders to obtain cash, goods or services for personal use is another common method of defrauding an employer. Skimming and larceny are other forms of employee fraud.

Skimming and Larceny

Skimming is the practice of removing money before it gets onto the books. Skimming can occur anywhere cash enters an organization, and businesses should be vigilant about ensuring that all cash handling procedures are secure.

- Sales skimming is when an employee sells goods or services without logging a sale and simply steals the cash. This usually shows up on a company's records as inventory shrinkage.
- Skimming receivables involves misappropriating payments before they are recorded. Because receivables skimming eventually shows up in a company's records in the form of delinquent accounts, a review of records can easily uncover the theft so dishonest employees often try to conceal their actions by forging, forcing or stealing account statements, destroying or deleting financial records, or by posting fraudulent write-offs.

Larceny is the physical theft of on-book cash**.** Most often cash larceny occurs when an employee steals cash from a bank deposit. Generally, skimming is much more common and costly than larceny,

Preventing employee fraud

The 10-10-80 rule of fraud states that 10 percent of employees will never steal; 10 percent will steal given the opportunity; and 80 percent will steal if they can justify the act in their own minds.

A critical first step in preventing internal fraud or theft at a company is to screen job candidates carefully. Besides verifying education, credentials, past employment and references, consider doing a criminal background check, a credit check and a driver's abstract scan. This is particularly important for prospective employees who will handle money, deal with financial matters or be responsible for company assets.

Beyond this, it is important to make it clear to employees that the company has zero tolerance for fraud or wrongdoing of any sort. Create and distribute a company policy that spells out exactly what constitutes fraud and specifies the consequences for it. A positive work environment, open lines of communication, and a fair grievance resolution mechanism can also help to mitigate employee fraud.

Accounting Controls

Firm, consistent internal controls will discourage most employees from attempting to steal. In addition, a system of checks and balances whereby business and financial functions are distributed and no single individual is responsible for billing, recording and processing transactions, preparing and making bank deposits, and reconciling statements is essential. Management should review APs and ARs frequently, verifying disbursements, payments and balances. Regular reviews and random audits will send a message to employees and also uncover any irregularities before they blossom into problems.

Internal Fraud Control Checklist

Actions that can be taken to reduce the likelihood of internal fraud include the following:

- Pre-employment background checks should be mandatory.
- Establish a zero tolerance policy for employee fraud, theft or dishonesty of any sort.
- Be clear with employees about what the company views as fraud. In addition to outright stealing, this may include misusing sick leave, doing substandard work, being habitually late or leaving work early.
- Have a written company policy that spells out consequences for internal theft, embezzlement, fraud or malingering.
- Do not allow any aspect of the business' finances to be handled exclusively by a single individual.
- Hold regular meetings to discuss issues and problems and establish a mechanism whereby employees can report employee theft anonymously.
- Conduct periodic surprise audits and have the books audited by an external third party twice a year.
- Be alert to disgruntled or stressed employees, or to those who may be having financial difficulties.
- Get an insurance policy that covers employee theft and fraud.

Unfortunately, it often takes a long time to uncover employee malfeasance. Most often it comes to light when an employee reports wrongdoing by a co-worker, or it is uncovered by accident.

Companies should adopt a proactive stance toward internal fraud rather than reacting to an occurrence that has been discovered. When internal financial resources lack the expertise or bandwidth to implement a fraud review and preventive guidelines, consider bringing in an external resource with expertise assessing the risk factors and recommending actions to prevent fraud-related losses.

About CFO Edge

CFO Edge is a leading Southern California provider of outsourced CFO services. Based in Los Angeles, we are a group of experienced chief financial officers who engage with CEOs and CFOs on demand to address strategic planning, business management, and day-to-day financial operations challenges. Our seasoned professionals deliver services as interim CFOs, part-time CFOs, project-based CFOs, recruitment-to-permanent CFOs and interim-to-permanent CFOs. At CFO Edge, we're passionate about helping our clients create, grow and sustain value. For more information, visit www.cfoedge.com or call 626.683.8840.

