Best Practices to Prevent Employee Fraud in a Recession

By Melissa Schwartz

Difficult economic times like these are always accompanied by an increase in employee fraud claims.

While most employees are honest and trustworthy burdened by financial stress, otherwise honest employees may be tempted to steal from their employers. At the same time, a tough economy is exactly when employers take a hard look at their operations to identify cost-cutting measures and often find that the numbers just don't add up.

Embezzlement and forged checks, as well as fraudulent bank accounts, expense reports and vendor invoices, impact companies of all sizes but for midsize and smaller companies, the criminal act can shut the doors forever.

Despite this threat, small and mid-size companies confronting a challenging business environment are often pressed to pare expenses. Funds that previously were invested in security measures or in the various types of insurance policies that absorb employee-related fraud exposures are invested elsewhere or simply conserved. However, it is at this time when companies should work even more closely with insurance brokers and carriers to transfer the risk of employee fraud rather than seeing insurance as an unnecessary expense.

Preventing Fraud

Fraud affects small-sized companies because there's often a high level of trust among management and staff, which elevates the confidence of the would-be perpetrators because they don't believe anyone would ever suspect them of fraud. Familiarity breeds a level of complacency that results in a higher susceptibility to fraud.

The following bullet points describe some best practices that companies can use to minimize fraud exposures:

- Segregate job duties so different employees reconcile bank accounts, write checks, and deposit money;
- Mandate finance staff to take paid vacations — often an employee perpetrating a fraud will forego time away from the office to ensure the scheme is not uncovered;
- Regularly scrutinize the veracity of the vendor list, and seek bids every three years from existing and new vendors;
- Conduct background checks of potential hires, and extensive examinations of individuals recruited for sensitive finance positions;
- Conduct regularly scheduled audits of protocols and processes, and spot audits that are unannounced until they occur;
- Work with insurance professionals to beef up anti-fraud measures and transfer remaining criminal risks to an insurance company.

These anti-fraud measures will also work well in combatting other factors raising the threat of employee criminal acts. For instance, cash conscious companies and non-profit organizations often are less apt to conduct extensive background checks on job prospects in their recruitment and hiring processes. Only after a crime has been committed do they learn that the employee had applied for the position under an assumed identity or had a criminal history of forging checks.

Midsize enterprises also tend to have weaker or limited process controls than larger companies, given the expense and impact on productivity. For example, they may not segregate employee duties because of a slim workforce. A single person may control an entire process, such as accounts payables and receivables, and only one person's signature may be required on company checks.

Smaller companies also are more likely to have blurred job responsibilities and few if any, checks and balances. Reporting responsibilities are confined to perhaps one person up the chain of command, and no one else is delegated the task of reviewing and evaluating the authenticity of financial transactions.

How It Happens

Fortunately, there are proven processes to decrease the risk of fraud by reducing the opportunity to commit it. The first step is becoming aware of some of the common areas at risk for fraud.

- *Forged checks.* Instead of depositing a customer's check in the company's bank account, the check is forged with the bookkeeper's name and then deposited in his or her account.
- *Fictitious vendor.* Employees can set up a fake vendor that provides "invoices" to the company. The employee will then mail a check off to the fictitious company or deposit the funds in the fake vendor's bank account.
- *Forged invoices.* Legitimate vendors can also be a vehicle to fraud with employees altering the amount on the invoice so that it is higher than the true amount, with the employee pocketing the difference.
- *Fabricate a fictitious or "ghost" employee.* This is most often committed by a payroll clerk who sends a salary check every week to the "employee," and then deposits the check in a bank account he or she controls.
- *Fraudulent expense reports.* An employee creates fictitious expenses that appear to be legitimate, but aren't. Company credit cards are a comparable example, used for personal and not business expenses.

Other white-collar crimes are less sophisticated but equally expensive, ranging from skimming money out of cash registers to the theft of expensive equipment like laptop computers and high-end furnishings or clothing. Even routine pilfering of company supplies can add up over time to big dollars.

Reducing a company's risk requires a mix of internal procedural changes, regular and ad hoc audits, clear policies forbidding fraudulent activities, and stringent penalties for employees caught in the act, including job termination and prosecution.

Working with insurance professionals can be of particular help to smaller enterprises, given their capital constraints and personnel resources. Specialized brokers and carriers are valuable partners in the fight against crime. Best of all, they can help these organizations purchase insurance policies that are right for their risk profile, with terms, conditions and financial limits that come into play.

Schwartz is vice president, management liability/fidelity, at Liberty International Underwriters in New York.