Employee Fraud

by: Kelly L. Frey, Sr. and Thomas J. Hall

U.S. businesses lose 5% of their revenues each year to fraud according to a new report issued by the Association of Certified Fraud Examiners (ACFE). In actual dollar losses, that translates to an estimated $652 billion, annually. Losses shared, unfortunately, within law firms as well as by our clients.

Fraud schemes by employees are especially troublesome and disproportionately affect small businesses. The ACFE study indicates that the typical occupational fraud scheme is difficult to detect (because of the extended time periods over which such fraud develops) and that small businesses (less than 100 employees) have higher losses per event than even the largest organizations (companies having over 10,000 employees).

Occupational fraud can take many forms, including:

- **Fraudulent financial reports**
- **Financial mismanagement by senior management**
- **Misappropriation of assets**
- **Making expenditures or incurring liabilities for improper purposes**
- **Obtaining assets or revenue by fraud**
- **Avoiding costs or expenses by fraud**

Or, in more familiar terms:

- **Cooking the books**
- **Padding the expense account**
- **Loafing**
- **Skimming**
- **Looting the till**
- **Sweetheart deals**

The most common form of employee fraud is misappropriation (i.e. theft or misuse) of company assets (which accounts for over 90% of reported fraud cases). Over 85% of such misappropriations involve cash. However, simply because cash is involved doesn't mean the amount of loss is small. In fact, the average loss in fraud involving cash is $150,000 (an amount that can be devastating to a small business). Most such cash frauds extend over months, probably based on the employee's assumption that "they'll never miss a little now and then.

Cash fraud can take the form of both "skimming" (stealing company cash before it is accounted for on company financial records) and "larceny" (stealing company cash after it is accounted for on company financial records). Such fraud can originate from billing (fraudulent or inflated invoices), expense reimbursement (fraudulent or inflated

expense reports), check tampering (forgery of a company check), payroll (false compensation claims), fictitious wire transfers, or false cash register entries.

Fraud can occur at all levels of the organization, but fraud losses tend to be highest in schemes committed at the highest management levels (including owners). Lower level employees were responsible for approximately 40% of the frauds studied, with the median loss from their actions being approximately $80,000. Managers also accounted for approximately 40% of the frauds in the ACFE study, but the median loss per incident was almost triple the employee frauds, averaging over $210,000 per incident. However, even though owners and executives accounted for the smallest number of frauds, losses from a scheme by an owner or executive averaged $1,000,000 per incident!

Two especially disheartening results of the ACFE study relate to the trust businesses place in long term and senior employees. The study concluded that there was a direct correlation between the length of time an employee had been employed and the size of the loss (with employees having ten or more years of employment responsible for median losses of $263,000 and employees with less than one year of employment responsible for median losses of $45,000). Similarly, the study concluded that while two-thirds of the reported frauds were committed by employees in the 31-50 age group, the largest losses to a business invariably resulted from frauds perpetrated by employees over the age of 60 (with loses from this senior group being almost 30 times greater than from losses from frauds committed by those 25 years or younger).

So how is a business to protect itself against fraud?

- Recognize that fraud is a very real exposure.
  Some people will steal without compunction, while others will steal under certain circumstances. Thus it is unlikely that any company will have a staff that is wholly immune to simple temptation, financial pressure, or both. As a result management must implement policies that deter misconduct. Simply focusing on detecting fraud after the fact is not a sufficient defense. Recovering lost funds or assets is difficult and time consuming, and the average recovery is only around 20% of the actual loss. In addition, fraud by an employee might create exposure to civil or criminal liability and cause significant harm to the company's reputation.
- Assess company operations to determine where opportunities for fraud exist.
  - Are blank checks kept in a secure location, or where theft can occur?
  - Are check writing machines secured, or readily accessible?
  - Does one person receive and deposit checks, approve invoices and issue payments?
  - Before you sign off on an invoice, how closely do you review the documentation?
  - What documentation do you require for an expense report?
  - Do you verify employment history and check references for new hires?
  - Do your employees believe they are treated, and paid, fairly?
- Institute, and enforce, internal controls to limit the opportunity for fraud, such as:
  - Reference checks for new hires
  - Separate financial responsibilities (e.g. do not give one person authority to deposit money, approve payments, and sign checks)
  - Never sign blank checks
  - Require, and review, documentation for all payment requests
  - Review and reconcile financial reports on a regular basis
  - Engage an outside financial auditor and conduct surprise audits from time to time
  - Consider using a third party payroll service
  - Use a "for deposit only" stamp on all incoming checks
  - Promptly and thoroughly investigate all customer reports that they have not received an order or have not received proper credit for a payment
  - Control access to blank checks and maintain an inventory of the supply on hand
  - Require that original invoices be kept in the files.

As the saying goes: "Trust, but verify." The goal is not complication for its own sake, but (i) to prevent fraud by making it difficult and (ii) to deter fraud by increasing the chances of early detection. For example, an employee contemplating a fraud against the company might not even bother attempting to cut checks to a fictitious customer if he knows a co-worker must also sign the checks and that the co-worker will insist on seeing the proper documentation. Even if the employee who is tempted to commit fraud has sole signing authority, he/she may hesitate if he/she knows the outside auditor may visit at any time.

Care should also be taken to protect the company against losses from kickback schemes or employee self-dealing. While the details of each kickback scheme may

Continued on Page 14 ➲

vary, such schemes tend to fall into two general categories:

- An employee sells an asset or service at a discount, in return for receiving something of value;
- An employee awards a contract, not to the lowest bidder, or to the best qualified vendor, but to the one that gave him/her a very large "gift."

In the first case, the company does not receive the full value of the service or asset sold; in the second case, the company will typically pay more than the going rate for the contracted goods or services. In each case, the employee profits at his/her employer's expense. Note that the employee receives "something of value," not necessarily cash in hand. Inducements can include trips to exotic locations, memberships, event tickets, and gifts of luxury items. As a result, it is recommended that companies prohibit personnel from accepting "gifts" of more than token value (e.g. pens, coffee mugs and the like), AND that the company publish this prohibition, and enforce it against both employees and the company's business partners (as a vendor may hesitate to offer a "gift" if it knows that it could be disqualified from further opportunities with the company).

While internal controls and external audits can be effective, the ACFE report clearly indicates that the most effective way to detect internal fraud is to establish an anti-fraud "tip line" where suspected fraud can be reported anonymously. In their study, the ACFE found that over half of all fraud was discovered as a result of such tips or by accident, rather than by any formal audit or through internal control processes. Anonymous tips were especially important in the detection of fraud by owner/executives and for the largest fraud losses (losses over $1 million). Encouragingly, the study found that over two thirds of all such "tips" actually originated with employees of the company itself.

While research indicates the value of such hotlines, merely waiting for the phone to ring is not sufficient to safeguard the company assets. Management should also be alert for the various "red flags" that often accompany employee fraud. These include:

- An employee living beyond his/her means
- Employee appears to have an unduly close relationship with particular vendor or vendors
- Frequent customer complaints about orders not received or failure to receive credit for payments
- Missing or altered documents
- Erratic employee behavior
- Secretive behavior (over and above what is needed to preserve business confidentiality)
- Apparent inability to handle money
- Failure or refusal to take time off

(as some frauds quickly come to light if the perpetrator is not on-site to cover the evidence on a daily basis.)

None of these, of course, is proof that an employee is defrauding his/her employer. They are, however, grounds for a closer look, which itself can offer two benefits:

- Discovering any fraud that may exist; and,
- Deterring potential fraud by demonstrating that management is vigilant and will not overlook "a little now and then."

Employee self-dealing can be a bit more subtle:

- Hiring friends or family over better qualified candidates;
- Steering work (or giving better terms) to friends, family or entities in which the employee has a financial stake.

Careful companies implement, and enforce, policies that prohibit nepotism and employee self-dealing.

When designing a fraud prevention program, some consideration should be given to the question of "when" and "why" employees will defraud their employers. As noted above, studies indicate that most persons are capable of fraud, in certain circumstances. Those circumstances appear to be a combination of financial pressure, the perception that the perpetrator won't get caught, and an ability to rationalize or justify the act. Of these, the employer has the greatest influence over the last two. Thorough controls, consistently applied, will do much to deter "casual" theft. Another effective deterrent is a happy work place, in which employees believe they are treated with respect and paid appropriately. Such employees are far less likely to dip into the till, while justifying to themselves that "the company owes me."

Fraud can create serious financial difficulties for any company. While internal policies and procedures can limit fraud, the ACFE study indicates that even the largest and most sophisticated business can be targeted by employees at the highest levels of the company. For small business lacking sophisticated audit and control processes, incidents of fraud may be even more prevalent (and the dollar losses, proportionately, even more devastating). But the good news is that a company's employees remain the best "policing agent" to detect fraud, and implementation of simple processes (such as internal controls and a "tip hotline") can be instrumental in discovering and reducing occupational fraud. ■

Kelly L. Frey *is a shareholder with the Nashville office of Baker Donelson Bearman Caldwell & Berkowitz, PC. He concentrates his practice in the area of corporate and information technology law. He can be reached at 615-726-5682 or kfrey@bakerdonelson.com.* ***Thomas J. Hall*** *is Of Counsel with the Nashville office of Baker Donelson Bearman Caldwell & Berkowitz, PC. He concentrates his practice in the area of corporate law and corporate procurement. He can be reached at 615-726-7302 or thall@bakerdonelson.com.*