Preventing Employee Theft is Simple; Spend a Little Time to Save a Lot of Money

By Nadine Swain

As a forensic accountant having analyzed hundreds of employee fraud matters, I have found among them a shared theme: all could have easily been prevented. Despite Hollywood portrayals, or the occasional Enron, the simple truth is that most frauds that affect businesses are, well, simple. This article details three concepts that provide the framework for fraud prevention. So, if your practice involves assisting startup companies, or consulting on business practices for established companies, sharing these concepts with your clients may go a long way in protecting their assets.

CONTROL THE CASH

The best way to prevent a fraud involving cash theft is to have a no-cash policy. While not practical for brick-and-mortar retail stores, service companies should give utmost consideration to a no-cash policy. For example, the majority of frauds I have investigated at doctors' offices involve an employee stealing cash from co-payments. A no-cash policy eliminates this problem at its root. In today's age of debit cards, PayPal, credit cards and the like, a no-cash policy would seemingly not affect most customers. If a no-cash policy is not practical, there are other options to control cash. First, companies should make it a practice to deposit all cash receipts several times per week, if not daily. Keeping cash on the premises serves as a magnet for filching employees.

Also, company owners, or a high-level employee, should review the bank-generated deposit tickets. A review of the deposit receipt will reveal red flags in the form of little or no cash deposits. I investigated a fraud in which the bookkeeper did not deposit a single cash receipt for months. The deposit receipts clearly told the story; had these been reviewed, it would have saved the company from losing six figures.

PERFORM COMPARISONS

In most cases of employee theft, the perpetrator takes steps to conceal the misdeeds. This typically involves manipulating the accounting records in some fashion. Thus, comparisons between the accounting records and other documents can stop an internal fraud in its tracks.

The employee theft scheme most often seen is lapping. Under this scheme, a person first removes cash from certain deposits. In order to restore the deposit to the appropriate level, the person replaces the misappropriated cash with an equal amount of checks. Accordingly, on any given day that lapping occurs, a comparison between what was posted to a customer's account, and the actual checks deposited, would reveal a discrepancy. The scheme would unravel from there.

Another employee fraud scheme involves an employee writing a check directly to him or herself. In these cases, the concealment usually involves doctoring the copy of the check image received with the bank's monthly statements. The comparison is best performed by matching the internal check copies with online images at the bank's website.

Similarly, comparing online check images with information posted in the accounting records is another simple way to stop or prevent theft. In some cases, a guilty employee will record checks payments, or company credit card charges, that appear to be legitimate business expenses in the accounting records. In actuality, the payment or charge may be completely different from what is reflected in the records.

LOOK FOR CLUES

Despite his or her best efforts, every dishonest employee leaves some sort of trail. Thankfully, most small businesses use an accounting software program. Even the most basic programs have built-in reports that reflect all activity. Reports such as "Audit Trails," "Exception Reports" and "Unusual Transaction Reports" potentially provide clues of employee theft. In fact, the IRS will frequently produce such reports during an investigation. Thieving employees will often engage in such activities as deleting sales, changing the method of payment, changing the sales amount and posting credits to conceal the misappropriations.

The general ledger provides a treasure trove of clues. With a weekly review of the general ledger, one can spot duplications and/or abnormalities. Recently, I reviewed a theft claim where the employee made unauthorized payments to herself. She attempted to conceal the situation by spreading the check amounts out across various vendors in the general ledger. A simple review of the ledger was enough to uncover a fraud that went undetected for two years.

So, in conclusion, if a business owner can employ the three simple concepts described in this article, the chances of losing assets to employee fraud are significantly reduced. The best thing is that they do not require much time or advanced accounting knowledge; so spending a little time can save a lot of money!

Nadine Swain is a certified public accountant. She is a at principal at Assurance Forensic Accounting, LLC, a firm providing financial damage measurement services for attorneys and insurance companies throughout the United States. The firm was named one of the fastest growing private companies in America by Inc. Magazine. You can reach Nadine directly at (706) 250-1119, or by email at nswain@assurancefa.com. www.assurancefa.com