How to Protect Your Small Business from Fraud

Publication	Bottom Line Personal
Original publication date	July 15, 2010

Workplace fraud siphons 7 percent of revenues from US organizations every year, and small- and mid-sized businesses are the most vulnerable. According to the Association of Certified Fraud Examiners, companies with fewer than 100 employees lost a median $200,000 to employee theft in 2008. Unfortunately, the culture of trust that knits a small and/or family-held business together can make their owners easy targets.

In the so-called "fraud triangle" that makes fraud possible, the perpetrator typically has a financial need (which is even more prevalent during these rocky economic times)... the ability to rationalize his/her deception... and an opportunity to commit fraud. Although you can't do much to eliminate the person's financial need or ability to rationalize, you can cut back on the opportunities...

• **Split accounting functions.** To help prevent employees from diverting payments that the business receives, make sure that the person who receives incoming payments isn't the same person who posts them to your accounting system.

• **Reconcile incoming payments daily** with the amounts that get posted to your books and deposited in your bank -- called *three-way reconciliation*. You or someone you designate should spot-check this procedure. If your bank gives you a desktop electronic check scanner, make sure that the device will credit funds only to your company's account. Otherwise, it's easy for an employee to scan in a check, direct it to a personal bank account, then shred the physical evidence and delete the check's image from your hard drive.

• **Guard your company's own checks.** Locking up your checks and placing strict limits on who may sign them can help discourage embezzlement, but these are just the first steps. Avoid signing blank checks ahead of a transaction, and never make a check payable to "Cash." Don't stock your business with erasable-ink pens, which employees can use to change the amount or the payee's name after you've signed. As for electronic transfers, although you can allow employees to set them up, you should review them in advance and only you should be authorized to send them out.

• **Monthly bank statements should be mailed either directly to your home or directly to you at work,** unopened, and you should review them right away. They should include images of all paid checks.

• **Pay close attention to merchant statements** from your credit card issuer for unusual deductions. Employees could use your card terminal to improperly transfer funds to their personal credit card accounts.

• **Outsource your payroll.** This is an inexpensive, hassle-free way to deter employees from tampering with your payroll. An outside service will perform the administrative chores and assume the compliance risks associated with the task -- all you do is call in your employees' hours.

The major services, such as ADP and Paychex, are reliable. In contrast, a smaller service needs to be monitored to make sure that it doesn't neglect to pay your federal and state payroll taxes on time.

Bottom Line/Personal interviewed Stephen Pedneault, CPA/CFF, founder of Forensic Accounting Services, LLC, an accounting firm in Glastonbury, Connecticut, that specializes in employee fraud. He is author of *Fraud 101: Techniques and Strategies for Understanding Fraud* and *Anatomy of a Fraud Investigation* and, most recently, *Preventing and Detecting Employee Theft and Embezzlement: A Practical Guide* (all from Wiley). www.ForensicAccountingServices.com