



Listen to this column on your computer or download and listen to it on your iPod or MP3 player at www.CPATechAdvisor.com/ColumnistsCorner.

For more information on aiding clients with technology issues, please visit:
 ▶ Helping Clients Find the Right Technologies: www.CPATechAdvisor.com/go/1876
 ▶ QuickBooks Data File Analysis: www.CPATechAdvisor.com/go/1513
 ▶ Troubleshooting Slow Multi-User Performance in QuickBooks: www.CPATechAdvisor.com/go/1145

Crime: Coming To a Business Near You

For the owner of a local engineering company, the mystery of the shrinking bank account was solved when one too many clients insisted that they had paid the owner's bill even though he'd never seen the checks deposited.

At a communications company that had recently relocated to the city, the slap in the face came when they discovered their office manager, whom they moved with them, had been writing a lot of checks to herself for more than a year.

And the technology services company got its first taste of employee crime when the VP was going through the last month's bank statement and found checks had actually been altered.

It's one of the ultimate acts of betrayal by an employee, but the number of companies victimized by someone they had trusted is clearly on the rise. The industry calls it occupational fraud. Call it what you want, but last year the crime wave cost U.S. companies more than \$990 billion (or 7 percent of revenue), according to the *2008 Report to the Nation on Occupational Fraud & Abuse* published by the Association of Certified Fraud Examiners.

The average loss for all businesses was \$175,000, but organizations with fewer than 100 employees fared the worst with a median loss of \$200,000. Some 40 percent of the victim companies were privately owned, and the crime (stealing) was carried out (on average) for nearly

- **Lockbox Processing:** Employees stealing cash and checks before they are deposited represents more than 10 percent of the occupational fraud. You can reduce that exposure by having customer payments delivered to a special post office box available only to your bank, which makes the deposits. This delivers on the tax and accounting professional inspired "separation of duties" process, but it has the side benefit of getting that cash into your bank account faster. Even better, many of today's accounting/ERP systems let you electronically transmit the lockbox deposit and automatically apply these payments to their corresponding invoices — a great time saver.

- **Biometric Time Clocks:** Claims for hours not worked and coworkers logging in for someone else show up high on the list of occupational

frauds. There can't be any so-called "buddy" punching if your time clock requires a fingerprint or handprint to enter time. This also stops honest employee from being pressured to become an accomplice by someone asking them to "clock me in."

- **Audit Trails:** Many accounting and ERP systems provide audit trails if you'll just turn them on. This feature keeps an electronic history with time and date stamps for data that is being changed in the system as well as the before-and-after values. Some systems even track data changes made directly to a Microsoft SQL Database, even if done outside the system. You now know who did what and when. Just remember these logs can get large, so only turn on what you need and make sure you have enough hard drive space.

- **Electronic Signatures:** This feature requires the user to authorize their identity for that specific process before they can change a data setup. Electronic signatures are also often used with Audit Trail features.

- **Safepay/Positive Pay:** Someone taking blank checks is an open door to do damage. With Safepay/Positive Pay, an electronic file showing all the authorized checks and amounts (as well as voided checks) is generated as part of every check run in the accounting system. The file goes to the bank, which won't honor a check until it confirms that the check number and the amount match the file. It's just like with a private party: If you're not on the list, your check is denied.

For all the hype about using technology (and often the hype is proven legitimate), there are times when the old fashioned methods can also be effective. Banks love it when you stop asking for your checks back because it is easier for them to send you copies of the scans. To make the point, they often charge a monthly fee for the trouble of returning checks to you. Sometimes, however, looking at tiny scans may cause you to overlook an obvious fraud. The technology services company cited above discovered it was a victim of fraud the first month it occurred because they had the physical checks returned from the bank, and the forgery on the check was plain to see. The key was opening the bank statements and spending 10 minutes each month actually looking at the checks. Catch the fraud early, and you've got a much stronger case for challenging the bank on why they cashed fraudulent checks. The technology company did just that, and the bank made good on the fraudulent checks.

For more information on fraud prevention, go to the Association of Certified Fraud Examiners' website at www.acfe.com. And very importantly, once you put your tools and processes in place, don't keep your fraud prevention checks and balances a secret. You want people to know you are watching. Prevention is the goal, and you definitely want to discourage those who might be tempted. ■



▶ DID YOU KNOW?

Earlier this year, the AICPA launched a new CPA specialty credential in forensic accounting. The credential, Certified in Financial Forensics (CFF), combines specialized forensic accounting expertise with the core knowledge of CPAs. The CFF encompasses fundamental and specialized forensic accounting skills in a variety of service areas, including: bankruptcy and insolvency, computer forensics; economic damages; family law; fraud investigations; litigation support; stakeholder disputes and valuations. To qualify, a CPA must be and AICPA member in good standing, have at least five years of experience in practicing accounting, and meet minimum requirements in relevant business experience and continuing professional education.

For more details, visit <http://fvs.aicpa.org/Memberships/Overview+of+Certified+in+Financial+Forensics+Credential.htm>.

two years before it was discovered. Check tampering and fraudulent billing was most common, and one-third of the time that criminal was in the company's accounting department. Most shocking? Only 7 percent of the perpetrators had prior convictions.

These are sobering statistics, particularly for a small company where occupational fraud has put many out of business. Before that happens to you or your clients, consider taking a bite out of the crime by taking advantage of the tools of technology to minimize risks.

- **Employee Screening:** It's a must in today's world, and it's never been easier. Ask applicants to sign the required release as part of their application process or when they've made it past the first round of interviews. With most screening services, you set up your account so you can enter information 24/7 on a prospective employee and get a credit report and driving record instantly or a criminal record check by the next day in your e-mail. The cost is minimal, and the insight into how the applicant has managed their personal life is very valuable. While not as technical, but just as important, you really should check those references and talk to past employers.