Small companies without adequate internal controls need CPAs to help them minimize fraud risk.

Protect Small Business

BY JOSEPH T. WELLS

■**SMALL BUSINESSES—ESPECIALLY THOSE** that do not have regular audits—have every reason to worry about fraud. According to a recent report, the per-employee losses from fraud in the smallest businesses are 100 times greater than those at their largest counterparts. Thus, this is an area in which CPAs can be valuable advisers to their clients.

■**CPAs CAN PROVIDE EMPLOYEE EDUCATION** with on-site fraud detection and prevention training, internal control reviews, cash reviews and reconciliations as well as inventory observations and asset verifications.

■**THREE MAJOR FACTORS CONTRIBUTE** to small business fraud: Inadequate employee prescreening—small businesses rarely spend money to check work references or records of potential hires; limited controls—the entity usually has insufficient personnel to adapt adequate controls; and too much trust—the very thing that makes a small organization a pleasant place to work also enables thieves within it to succeed.

■**ASSET MISAPPROPRIATION AND CORRUPTION,** two common forms of small business fraud, are areas in which CPAs can train owners and employees to spot the red flags that signal wrongdoing inside their company.

■**CPAs ALSO CAN EDUCATE THEIR CLIENTS** about theft coming from outside the company in the form of check fraud, credit card fraud and bust-outs, which are schemes where customers will purposely buy huge amounts of merchandise and run up debts they have no intention of paying.

JOSEPH T. WELLS, CPA, CFE, is founder and chairman of the Association of Certified Fraud Examiners and a professor of fraud examination at the University of Texas at Austin. Mr. Wells is a member of the AICPA Business and Industry Hall of Fame. He won the Lawler Award for the best *JofA* article in 2000. Mr. Wells' e-mail address is joe@cfenet.com.

Denise, a bookkeeper for a small trucking firm in Birmingham, Alabama, wishes she had never heard of Ralph Summerford, CPA. Because of his thoroughness, Denise is facing several years in prison for embezzling $550,000 from her employer. At least she will look good standing before the the sentencing judge: Denise spent a great deal of her illegal loot on head-to-

toe cosmetic surgery. She blew the rest on a shiny new Lexus, luxury vacations, clothing and jewelry. And, of course, Denise had to have a big house to store all of her finery.

Surprisingly, it wasn't the high living that made her employer suspicious. "The owner was going over the trucking company's budget when he noticed Denise's salary was listed at $38,000 a year," said Summerford. "But the business owner distinctly remembered that he had set her pay at $35,000." The owner pulled Denise's personnel file and discovered that someone had altered her pay record. It was obvious to him that no one but Denise would have been motivated to falsely increase her salary. Investigating further, he noticed suspicious-looking wire transfers from the company's bank account. That's when he called in Summerford.

"Like a lot of small businesses, the trucking company had very limited accounting controls," said the veteran CPA, now a partner with Dixon Odom PLLC in Birmingham, Alabama. "In this case, the sole division of responsibilities concerned authorizing all the checks. While only the owner could sign checks, Denise did everything else: post the books, reconcile the checking account and authorize wire transfers."

Her scheme was simple. After wiring money directly from the company bank account to her own, Denise would post the books, charging the funds transfer to one or more expense accounts. Then, when she reconciled the bank account, she simply would tear up the evidence. Summerford investigated the fraud case, interviewed Denise's coworkers and assembled the documentary evidence including bank statements, wire transfer requests and deposit slips. He then prepared charts and exhibits summarizing the scheme, which he included in a written report to prosecutors. Summerford's work was used to indict Denise for her thefts.

"Denise was well aware the owner did not review the bank statements," said Summerford, also a certified fraud examiner. "And since the business was not audited, there was no independent review of Denise's work; yet almost any degree of scrutiny of the bank statement could have prevented this scheme."

Summerford said most schemes like Denise's start out relatively small. "But when thieves avoid detection, it motivates them to steal even more," he said. "Many will continue to steal from a small business until it literally runs out of money and goes broke."

Although the trucking company didn't go bankrupt, Denise's thefts were extremely costly. Small organizations face a serious fraud problem: Dishonest employees will steal them blind.

There's Nothing Small About Small Business

Studies show small businesses

■Account for **58%** of the nonfarm workforce.

■Contribute to **43%** of all sales in the country.
■Generate **51%** of the private gross domestic product.

Source: www.sba.gov.

BIG CONCERN FOR SMALL BUSINESS

Small businesses have every reason to worry about fraud. According to the Association of Certified Fraud Examiners' (ACFE) "2002 Report to the Nation on Occupational Fraud and Abuse," the per-employee losses from fraud in the smallest businesses are 100 times the amount of their largest counterparts. (The complete report can be downloaded at www.cfenet.com.) Thus, this is an area in which CPAs can be valuable consultants to their clients. Most small businesses don't have a need for a CPA to do a full audit; however, CPAs can provide a number of fraud prevention services.

■***Employee education.*** CPAs can conduct on-site training for clients in the form of live presentations and/or computer-based education.

■***Internal control reviews.*** Reasonable internal controls are critical in a small business. A CPA can review the existing system and make recommendations for improvements.

■***Cash reviews and reconciliations.*** Since 9 in 10 occupational frauds involve the company's cash, CPAs can regularly review receipts and disbursements for anomalies. Although this is an excellent deterrent, it's important to realize that no CPA can guarantee that any specific procedures will uncover fraud.

■***Inventory observations and asset verifications.*** For companies with inventory or other assets that make attractive misappropriation targets, CPAs can observe inventory procedures and/or verify specific items. Both the 1996 and the 2002 ACFE study showed a similar trend: Small business is very vulnerable to fraud. There appear to be three reasons.

■***Inadequate employee prescreening.*** Small businesses rarely spend the money to check work references, criminal records or professional recommendations of potential hires or require applicants to undergo drug screening, psychological testing and other vetting procedures. Undesirable applicants know this and thus gravitate to small businesses. The problem, according to the study, is that about 7% of employees have a history of workplace theft and fraud. This small but costly group knows the degree of scrutiny into their past likely will be minimal; all too often, they are right.

■***Limited controls.*** The bedrock of fraud prevention is the division of responsibilities between employees. The reason is straightforward enough: It is one thing to steal by yourself but quite another to enlist the aid of a coworker. Small businesses rarely have sufficient personnel to adapt adequate controls; "one-person accounting departments" as in Denise's case are the rule, not the exception. Consequently, it becomes

important for the owner to overcome this deficiency with reasonable oversight, which can be accomplished two ways. First, the business owner should actively understand and verify the financial information reported to him or her. Second, the owner can engage a CPA to attest to the credibility of the financial information, even if the company doesn't have a regular audit. However, the audit can be a powerful deterrent in its own right: The ACFE study found losses to companies that had audits were about a third lower than losses at companies that didn't.

■***Too much trust.*** The third factor for large fraud losses in small businesses involves the human element. In a situation where employees know each other well, it is natural for them to trust one another. Indeed, the intimate familial atmosphere of a small business is one of its most appealing features. Most of the time, believing in your coworkers is well founded, but not always. The dichotomy is that trust is an essential element of business as well as an essential element of fraud. Never having faith in your employees is a bad thing; so is always trusting them. The goal is to strike a balance between the two. Or, as Mark Twain said, "Trust everybody, but make sure you cut the cards."

OCCUPATIONAL FRAUD SCHEMES

Small businesses are most vulnerable to two types of fraud from within: asset misappropriation and corruption. Moreover, according to the study, the average length an occupational fraud goes on before discovery is about 18 months. By recognizing the common warning signs or red flags of these schemes early, businesses can reduce or avoid losses. Fraud indicators include: rising expenses and/or declining revenue, abnormally high inventory shrinkage, unfamiliar vendors or other payees and excessive spending by employees. Moreover, studies have shown that employees who engage in workplace abuse (excessive absenteeism, goldbricking, pilfering, for example) are at a higher risk to commit fraud.

Isabel Mercedes Cumming, a prosecutor in Baltimore, is a former internal auditor. "We see a great deal of fraud cases involving workers in small businesses," she says. "Most of them involve employees stealing money or merchandise, and some cases involve hundreds of thousands of dollars. In my view there often is a certain naiveté on the part of small business owners who fail to recognize that employees can and do commit fraud. Many of these offenses could be avoided altogether if the owners were alert to the risk and took reasonable internal control measures. Simply stated, small business owners tend to place too much trust in their employees."

ASSET MISAPPROPRIATION

The definition of *asset misappropriation* is broader than simply theft; an employee who uses the company computers at night to run his or her own side business has not stolen the computers, but certainly something of value has been misappropriated (see "Enemies Within" *JofA*, Dec.01, page 31). Although a crooked employee can misappropriate any company asset, these schemes can be broken down into two major classifications: cash and noncash.

Cash. As a CPA adviser to a small business, ask this question: "If an employee could steal any asset, which one would it be?" In 9 out of 10 cases, the answer is obvious: cold, hard cash. The reasons are equally apparent. A thief working for a test-tube wholesaler would need to fence the illegal bounty on the black market; a dishonest

employee working in the coal mines would need to pilfer tons of the stuff to do any good. But like Denise, everyone spends money. Any enterprise's cash is vulnerable in three areas.

■***Skimming.*** Skimming involves a crooked worker stealing money from the business before it is received and recorded by the company. The usual culprits are salespeople and accounting department personnel. They filch money that should be credited to sales or accounts receivable (see "…And One for Me" *JofA*, Jan.02, page 90 and "Lapping It Up" *JofA*, Feb.02, page 73).

■***Larceny.*** Larceny is the theft of currency after the company has received and recorded it. The employee usually is a cashier or someone with easy access to currency. Because currency is generally closely watched, these schemes are infrequent and relatively inexpensive.

■***Fraudulent disbursements.*** The most expensive cash frauds relate to fraudulent disbursements from a company's bank account. Employees in the accounting or bookkeeping department are in a position to cook up these schemes. In a typical case, the employee submits a false invoice the company unknowingly pays to the benefit of the thief. Fraudulent billing most commonly involves services that are not rendered to the company. The employee usually conceals illegal payments by having checks made out to friends, relatives and shell companies. In Denise's case, because of a complete lack of oversight, she didn't even have to bother with phony paperwork. (See "Billing Schemes, Part 1: Shell Companies That Don't Deliver" *JofA*, Jul.02, page 76; "Billing Schemes, Part 2: Pass-Throughs" *JofA*, Aug.02, page 72; "Billing Schemes, Part 3: Pay-and-Return Invoicing" *JofA*, Sep.02, page 96; and "Billing Schemes, Part 4: Personal Purchases" *JofA*, Oct.02, page 105.)

Noncash. Although any other asset of the business is up for grabs, crooked employees usually opt to steal something that is particularly useful to them personally. Consumer goods such as clothing, groceries, electronics and jewelry are favorites. Office supplies and equipment (laptop computers, handheld devices, software and calculators) top the list of hard assets likely to be stolen.

CORRUPTION

A less common but much more expensive occupational fraud involves a corrupt employee who conspires with someone outside of the company. For example, purchasing agents and buyers are constantly barraged with offers of free trips, gifts and other enticements by vendors attempting to curry favor. Sometimes these situations turn into outright graft. However, the victim company actually pays the bribe in the form of higher prices or substandard goods and services that the vendor delivers; widgets costing $100,000—which includes a $20,000 kickback—can be purchased on the open market for $80,000 or less.

PREVENT AND DETECT INTERNAL FRAUDS

In addition to the other methods discussed here, CPAs should advise their small business clients about measures to help prevent and detect internal fraud.

Education. Employees are the eyes and ears of small business; if something is amiss, they likely will know about it before management or the auditors. Their education

should concentrate on three areas: why fraud occurs, how to recognize it and what to do if they suspect fraud. The AICPA and the ACFE, as a public service, have jointly produced a free one-hour interactive training program that can be used to educate employees about fraud. CPAs can download it from the AICPA Web site at www.aicpa.org/antifraud/training/homepage.htm.

Active oversight. The company's principals need to learn about schemes, too, to be involved in fraud prevention in their companies. Above all, the owner should receive an unopened bank statement so he or she can review it for suspicious transactions. Moreover, the principals need to ensure they understand the entity's revenue and expense streams so they will be able to notice unusual trends.

Reasonable personnel policies. Employees are much more likely to steal from businesses when they perceive they are being treated unfairly or think the business owner is deceptive. In addition to setting the proper example, owners need to make sure they treat employees well and reasonably compensate them. Otherwise, employees might attempt to right their grievances with not only unproductive behavior, but with fraud and theft, too.

Seek professional assistance. When an enterprise has serious questions about fraud prevention and detection, the CPA should advise the owners or principals to seek professional assistance from a CPA/CFE fraud specialist or from some other qualified expert.

THIEVES OUTSIDE THE DOOR

Although historically occupational frauds have been more expensive than white-collar crimes, the rise in the latter points to an increase in crooked customers, vendors and other outsiders. Small businesses are vulnerable in several key areas.

Check fraud. Since the late 1980s, check frauds have grown markedly. As nearly any merchant can tell you, accepting a forged, stolen or counterfeit check is commonplace. A major cause has been the development of laser printers and desktop printing equipment; the tools necessary to pull off this crime are easily and cheaply available at the neighborhood computer store. Another reason for the rise in both check—and credit card—fraud relates to the current wave of identity fraud. Crooks have discovered that it is relatively easy to get a completely fictitious name and the accompanying identification that is necessary for the scheme's success. With false ID, the ocean of commerce is the fraudster's pearl. He or she can open up bank accounts, obtain credit cards, buy property, incur debt, get passports, open offshore accounts—you name it. The best defense to identity fraud is for small business personnel to know their customers. The second-best defense is to train employees who accept checks to be alert to some common signs.

■Counterfeit checks are frequently of poor print quality. Only government checks have smooth edges on all four sides—any other legitimate check will have one perforated edge.

■The signature on a forged check will often extend past the signature line since the forger usually has limited experience writing someone else's name.

■New bank accounts are more prone to fraud than established ones. Before accepting a check, an employee should note whether the date the account was opened is listed on the face of the check. If so, he or she should be cautious in accepting checks from an account less than 6 months old.

■Be wary of checks with a number less than 200.

Credit card fraud. Although small businesses are victims of a wide variety of credit card fraud, most of the schemes can be divided into four types: stolen credit cards; identity fraud, which occurs when the card is issued to a user in someone else's name; altered credit cards, changed by flattening the alpha/numeric characters and reembossing them with different identifying information; and counterfeit cards. While some counterfeits and altered cards are undetectable to the naked eye, many more are crude look-alikes. Employees should be alert to

■Holograms badly faked with tiny bits of aluminum foil.
■Misspellings on the card.
■Alterations on the signature panel.
■Discolored, glued or painted cards.
■Cards that appear to have been flattened and restamped with different numbers.

Aiding in the success of these schemes is the fact that, according to a study by *Money* magazine, 95% of U.S. cashiers did not verify credit card signatures by comparing them with those of the customers. Like check frauds, the front line of defense in credit card frauds is employee education, which should include awareness of customer behavior. Employees handling credit cards should know that crooked customers frequently display certain characteristics such as

■Taking a credit card from a pocket instead of a wallet or purse.
■Purchasing an unusual number of expensive items.
■Making hurried or random purchases, with little regard to size, quantity or value.
■Making several large purchases under the approved limit or asking an employee what the limit is.
■Charging expensive items on a newly issued card.
■Signing their names on the sales receipt slowly or awkwardly.

BUST-OUTS

For small businesses with their own charge accounts, CPAs should alert owners and employees to the risk that some customers will purposely buy huge amounts of merchandise and run up debts they have no intention of paying. This type of fraud is called a "bust-out" and usually is committed by newly established commercial enterprises. These "front" businesses normally start off charging small amounts, paying on or ahead of time in order to establish creditworthiness, and then ordering large quantities of inventory on credit. They subsequently sell the inventory at deep discounts, and the fraudsters avoid payment by one of two methods: They pull up stakes and disappear from sight or they file for bankruptcy.

Ten Ways Small Business Owners Can Prevent/Detect Fraud

1. Hire a CPA to examine the books.
2. Have a written code of ethics.

3. Set a good example.
4. Have reasonable expectations.
5. Treat employees well.
6. Restrict bank account access.
7. Perform regular bank reconciliations.
8. Adequately secure inventory and supplies.
9. Adequately prescreen employee applicants.
10. Give employees a way to report fraud.

Robert DiPasquale, a CPA and certified fraud examiner with Videre Group in Parsippany, New Jersey, says bust-outs also can be used to acquire a business. In one case, he was hired to investigate the sale of a family-owned retailer of baby furniture.

"The business had been in the family for generations. When one of the sons inherited it, he decided to sell," said DiPasquale. "The buyer paid a small sum as a down payment with the seller financing the balance. After about a year, the payments to the seller stopped. Ultimately, the seller filed a lawsuit to recover the remaining inventory and other assets, but they were long gone."

As a result of the lawsuit, the buyer of the store filed for both personal and business bankruptcy protection. That turned out to be a mistake when DiPasquale was retained to review the buyer's books and records. DiPasquale was able to assemble evidence that indicated the buyer had purchased the business with the intent of defrauding the seller.

"We found out that immediately after the purchase of the business, the buyer began ordering large quantities of inventory that were later moved off-site and sold at huge discounts. Moreover, the buyer was skimming the store's sales for himself," DiPasquale said. DiPasquale's work resulted in both bankruptcy petitions being overturned. The court ordered the buyer to repay the seller the entire sales price with interest.

To avoid becoming the victim of a bust-out, train employees to
■Be cautious in extending credit to new commercial enterprises or unknown parties.
■Look for early repayments of small amounts followed by charges of increasingly larger amounts.
■Be alert to businesses that use a post-office-box address or are not listed in the telephone book.
■Check with the police or the Better Business Bureau if you are in doubt about the legitimacy of a charge account customer.

INTERNET AND COMPUTER FRAUDS

Although the Internet and the computer have been a boon to small businesses, this progress has not come without a price. Computer hacking, viruses and spamming have become ordinary, everyday business events. And according to Sandra Johnigan, a Dallas CPA and chairperson of the AICPA's litigation and dispute resolution subcommittee, small businesses are particularly at risk of computer-facilitated crimes. "Moreover, there is a growing trend of employees' using the company's computer to run their own businesses," Johnigan observed. She said that dishonest employees also

might steal their employers' technology, customer lists or other business secrets in order to set up a competing enterprise. CPAs should advise their clients to take adequate security measures to protect the company's secrets, including ensuring that sensitive documents are shredded or otherwise rendered unreadable before they are discarded.

With limited personnel, small businesses frequently must compromise on the division of responsibilities. Nonetheless, to keep employees on the straight and narrow, managers should attempt to assign separate workers to the functions of data entry and asset control. In the simplest terms, an employee who controls records should not control assets and vice versa.

Johnigan said that conducting business on the Internet usually is a safe proposition when accompanied by a few basic security procedures. Last year, the White House released a draft report for small business to be mindful of cybersecurity and to consider five simple steps to reduce risks of fraud.

■Use a tough password of at least eight digits, with a mix of numerals and uppercase and lowercase letters.
■Maintain an updated virus protection program.
■Install update "patches" (that is, check software company Web sites for improvements to existing security).
■Use filtering techniques.
■Use firewalls in computers that have "always on" broadband connections.

ADVISE, EDUCATE AND STAY ALERT

Fraud is a cost of doing business that is hidden from view. We know about frauds only when they are discovered, and then it sometimes is too late to do anything to avoid catastrophic losses. The first line of defense is a CPA who advises business owners about fraud prevention and detection techniques. These include hiring the right employees—people with no known history of dishonesty—and treating them fairly. Employers and workers need to learn about fraud and how to report it, and CPAs can greatly assist small businesses by providing such antifraud services. Eliminating fraud completely is not possible, but with reasonable measures, its impact can be limited. Preventing fraud from occurring in the first place, however, is the only win-win situation. ■

Resources on Internet and Computer Fraud

Web sites

Federal Trade Commission
www.ftc.gov
This site contains a great deal of information regarding consumer protection and fraud.

National Fraud Information Center
www.fraud.org
This site is operated by the National Consumers League in cooperation with the National Association of Attorneys General and the Federal Trade Commission. Its Internet Fraud Watch area offers guidance on how to recognize and avoid Internet hoaxes and provides incident reporting forms for victims, as well as statistics on Internet fraud.

Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice
www.cybercrime.gov
The CCIPS has information about computer crimes, encryption, electronic commerce, hacking, legal issues relating to cybercrimes, privacy issues and international issues.

Computer Security Institute
www.gocsi.com
CSI provides training for information, computer and network security professionals. It conducts its annual "Computer Crime and Security Survey" in conjunction with the FBI.

U.S. Postal Service
www.usps.gov
The Postal Inspectors' section of this site has great information concerning mail fraud and other types of fraud involving the postal system.

Internet Fraud Complaint Center
www.ifccfbi.gov
The IFCC is a partnership between the FBI and the National White Collar Crime Center. It provides information about Internet fraud as well as a reporting mechanism that alerts authorities of a suspected criminal or civil violation.

Books

Avoiding Cyberfraud in Small Business: What Auditors and Owners Need to Know, Jack Bologna and Paul Shaw, John Wiley & Sons, New York, 2000.

How to Prevent Small Business Fraud: A Manual for Business Professionals, Association of Certified Fraud Examiners, Austin, Texas, 2002.