

# How to *Steal* from a Nonprofit: Who Does It and How to Prevent It

by Janet Greenlee, Mary Fischer, Teresa Gordon, and Elizabeth Keating

Payroll and check  
tampering fraud  
were more common  
in the nonprofit  
sector than in the  
business sector.

**Editors' note:** This article was written as a working paper for the Hauser Center for Nonprofit Organizations at Harvard University. It has been adapted and published in collaboration with the editors of the Nonprofit and Voluntary Sector Quarterly. Readers can access the full article in the December 2007 NVSQ at <http://nvs.sagepub.com>.

IS IT EASIER TO STEAL FROM A NONPROFIT organization than from a business? That's what some researchers have speculated, arguing that an atmosphere of trust, the difficulty in verifying certain revenue streams, weaker internal controls, a lack of business and financial expertise, and a reliance on volunteer boards all contribute to increased nonprofit vulnerability.

To identify how people steal from nonprofits and how to prevent it, we turned to the biannual surveys of fraud examiners. In its *Report to the Nation on Occupational Fraud and Abuse* published in 2005, the Association of Certified Fraud Examiners (ACFE) focused on both internal and external fraud. In all, it studied in depth 508

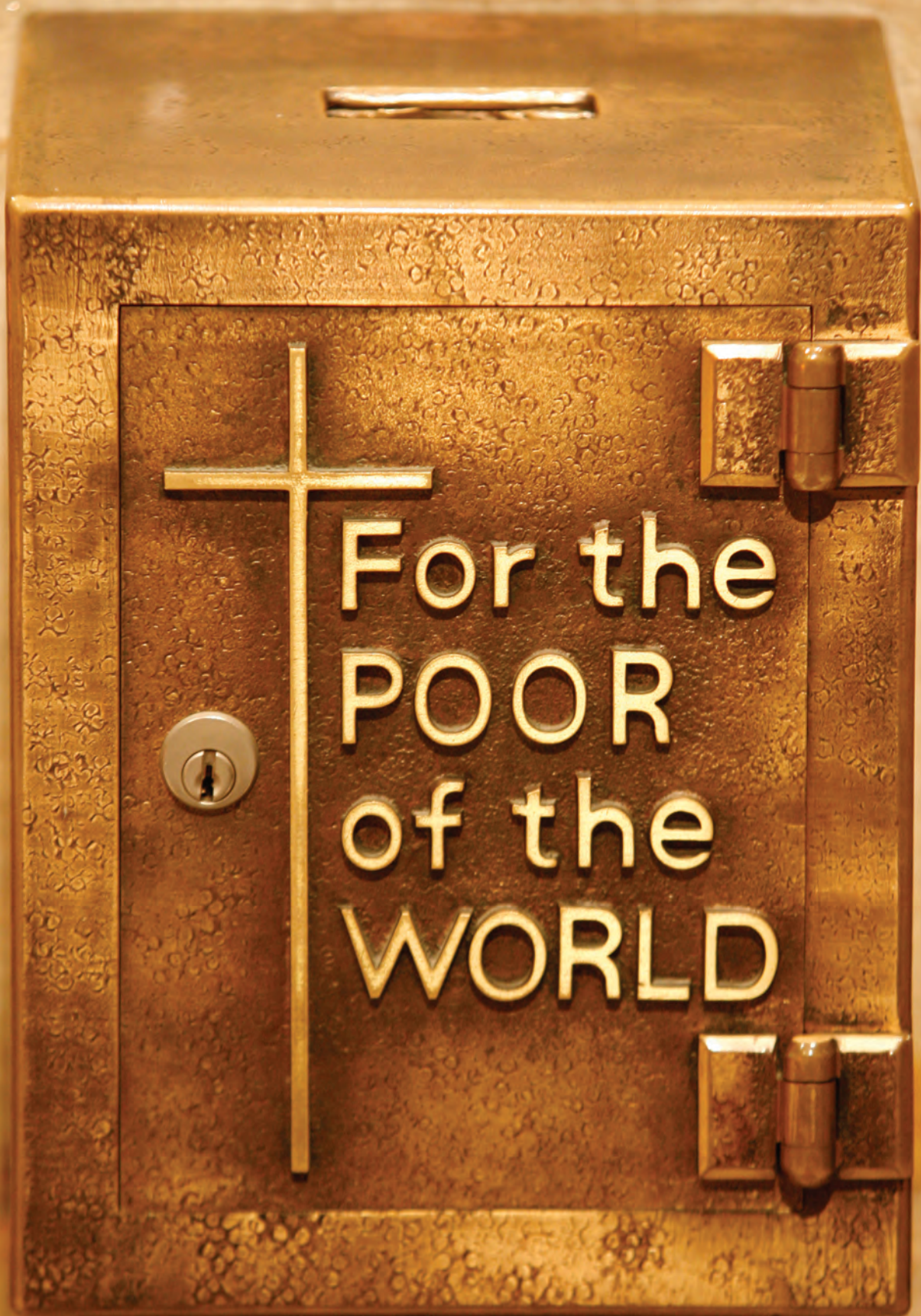
cases of occupational fraud representing \$761 million in losses. In segregating its findings by sector, ACFE's 2005 report enables us to draw some lessons and comparisons specifically related to nonprofits.

Of the 508 occupational fraud cases reported by ACFE members, 58 or 12%, occurred in nonprofit organizations (see Table 1). In the case of Enron, WorldCom, and other for-profits, the primary underlying offense was misrepresentation of financial information to investors, regulators, and the public. In contrast, nonprofit crimes tend to involve the less complex unauthorized taking of funds for personal use. But when you look at the median losses per incident, they are strikingly similar to losses suffered by businesses and significantly higher than those suffered by government. According to the report, fraud losses in the 58 nonprofit cases ranged from a low of \$200 to a high of \$17 million, with a median loss of \$100,000.

The ACFE survey found that both payroll and check tampering fraud were more common in the nonprofit sector than in the business sector, while false invoices and skimming from revenues were

---

**JANET GREENLEE, PH.D., CPA**, is an associate professor of accounting at the University of Dayton in Ohio. **MARY FISCHER, PH.D., CGFM**, is a professor of accounting at the University of Texas at Tyler. **TERESA P. GORDON, PH.D., CPA**, is a professor of accounting at the University of Idaho. **ELIZABETH K. KEATING, PH.D., CPA**, is a visiting assistant professor at Boston College and an associate scholar at the Urban Institute.



The typical nonprofit fraud case was committed by a female with no criminal record. She earned less than \$50,000 a year and had worked for the nonprofit for at least three years.

more prevalent in for-profit entities. Four of the 58 nonprofits realized losses of more than \$1 million, while an equal number of organizations experienced losses of \$2,000 or less.

### Who Commits Fraud?

According to ACFE's study, the typical nonprofit fraud case was committed by a female with no criminal record. She earned less than \$50,000 a year and had worked for the nonprofit for at least three years.

More than 25 percent of the reported nonprofit frauds were conducted by managers, while 9 percent of the perpetrators were executives. Organization managers committed fraud that resulted in the greatest median loss to the organization (\$150,000). The most costly frauds were those perpetrated by male managers and executives earning between \$100,000 and \$149,000 per year.

The perpetrators' ages ranged from 20 to 62, with a median age of 41. Median tenure with the organization was seven years but ranged from less than one year to 35 years.

Perpetrators who had been with the organization for more than 10 years generated a median loss of \$230,000, but the greatest losses were generated by those who had been with the organization the longest; they were between 51 and 60 years old, and their median loss was \$257,000.

While only 19 percent of the frauds involved collusion (i.e., the involvement of more than one person), the median loss for frauds involving collusion was more than four times that of frauds perpetrated by a single individual. As part of the survey data gathering, respondents were asked to disclose the criminal history of the perpetrator(s). Most perpetrators had not been charged with or convicted of any crime prior to the fraud, and the size of the loss was not correlated with a criminal background.

### What Do Various Types of Fraud Cost?

In *Principles of Fraud Examination*, among the three types of occupational fraud (i.e., asset misappropriation, corruption, and financial statement fraud), author Joseph T. Wells found that asset misappropriation made up more than 97 percent of all reported frauds.<sup>1</sup> Nonprofit organizations in the ACFE study also cited misappropriation as by far the most common type of fraud. Financial statement fraud was the least

common, representing only 5 percent of the nonprofit sample. However, the \$3 million median loss from these cases was 30 times the \$100,000 median loss from asset misappropriation.

Almost 95 percent of all reported asset misappropriations involved cash, with a median loss of \$100,000, and these cases involved skimming, larceny, and fraudulent disbursement. More than 75 percent of cash misappropriations involved fraudulent disbursements (when an organization pays an expense that it does not owe). Skimming occurs when cash is stolen *before* it is recorded. Larceny takes place when cash is stolen *after* it is recorded. Fraudulent disbursements are associated with median losses of \$145,000, while skimming, which represented 22 percent of the sample, had a smaller median loss of \$40,000.

Since the majority of cash misappropriation involves fraudulent disbursements, the ACFE survey asked respondents to identify losses by type of fraudulent disbursements. There are five major types of fraudulent disbursement transactions: (1) fraudulent billing occurs when false or inflated invoices are paid; (2) payroll fraud occurs when a payroll check is issued based on overstated hours worked or to fictitious "ghost" employees; (3) expense reimbursement fraud occurs when falsified claims for expenses are submitted by employees for such things as travel reimbursement; (4) check tampering occurs when an organization's check is stolen or altered; and (5) fraudulent register disbursements occur when false entries are made in a cash register or cash refunds are made from the register without documentation.

Fraudulent billing is the most common type of fraudulent disbursement, comprising almost 50 percent of the total. But the most costly fraud involves register disbursements, with a median loss of more than \$350,000. The least costly type of fraudulent disbursement is expense reimbursement, with a median loss of \$83,373.

In the business sector, fraudulent financial statements have been widely publicized, which in 2002 led to passage of the Public Company Accounting Reform and Investor Protection Act, also known as the Sarbanes-Oxley Act. Typically, financial statements are falsified by one or more of the following: (1) overstating revenues, (2) understating liabilities or expenses, (3) recognizing revenue or expenses in the wrong period, (4) reporting assets at either less or more

than the actual value, and (5) failing to disclose significant information. Fraud examiners reported three cases of fraudulent nonprofit financial statements. Overstating revenues resulted in the largest loss, at \$10,000,000. Inappropriate asset valuation and lack of disclosures both resulted in \$100,000 losses.

# Uncovering Crimes

How was fraud discovered? Contrary to what some might believe, it was relatively rare for fraud to be discovered via the audit process. More than 86 percent of the sample organizations had undergone external audits, which is much higher than the rate of audits experienced by the overall nonprofit population.

More than 43 percent of the frauds were detected by tips, with half of these tips coming from employees, while only a quarter of the frauds were detected by the internal audit department. Tips from vendors led to detection of the frauds with the greatest losses. Frauds detected through customer tips were the smallest, with a median loss of \$2,600. More than 22 percent of the reported frauds were caught by accident, while only 12 percent were found by an external auditor. Internal controls were credited with helping to detect nearly 14 percent of the cases.

Although internal controls and internal and external audits were useful in identifying a third of the fraud cases, nonprofit organizations that had undergone internal or external audits did not see a reduction in the size of their fraud losses.

# Are People Held to Account?

When a fraud is discovered, an organization can charge the perpetrator(s) criminally and/or civilly. Seventy-two percent of the nonprofit frauds resulted in termination, but 7 percent resulted in no punishment. In comparison, for-profit fraudsters were more likely to be terminated (88 percent) but had an equal chance of not being punished (7 percent).

This does not mean that employers necessarily retained the fraudsters. In many cases, it was reported that the perpetrator quit or disappeared when his scheme was discovered. Not surprisingly, large losses were more commonly referred to law enforcement for criminal prosecution (72 percent). The median loss related to frauds reported to the authorities was \$140,000 as compared with just \$6,700 when no criminal referral

| Table 1. Organizational Victims of Fraud with Median Dollar Loss   |                                      |                        |
|--|--------------------------------------|------------------------|
| Type of organization   | Percentage of the 508 reported cases | Median loss from fraud |
| Private company  | 41.8                                 | \$123,000              |
| Public company   | 30.2                                 | \$100,000              |
| Government agency  | 15.8                                 | \$37,500               |
| Nonprofit organization   | 12.2                                 | \$100,000              |
| Source: Association of Certified Fraud Examiners (ACFE), Report to the Nation on Occupational Fraud and Abuse, 2005. |                                      |                        |
| Table 2. Characteristics of the Victims and Perpetrators of Fraud in Nonprofit Organizations in ACFE Study           |                                      |                        |
|  | Mean                                 | Median                 |
| Number of employees  | 4,606                                | 58                     |
| Age of organization  | 40.2                                 | 30                     |
| Number of perpetrators involved  | 1.6                                  | 1                      |
| Age of principal perpetrator   | 41                                   | 41                     |
| Tenure with organization of principal perpetrator  | 7.4                                  | 4                      |
| Total dollar loss caused by fraud  | \$535,104                            | \$100,000              |
| Source: Association of Certified Fraud Examiners (ACFE), Report to the Nation on Occupational Fraud and Abuse, 2005. |                                      |                        |

More than 43 percent of the frauds were detected by tips, with half of these tips coming from employees, while only a quarter of the frauds were detected by the internal audit department.

was made. Of those cases resulting in criminal prosecution, 70 percent of the accused individuals pleaded guilty or no contest and five were acquitted.

Finally, survey respondents were asked whether a percentage of the loss was recovered. Fifty percent recovered nothing, with a median loss of \$95,873. Thirty-four percent completely recovered their loss (median loss of \$25,350). Insured organizations recovered about 57 percent of their loss.

# Predicting and Preventing Fraud

According to W. Steve Albrecht, a leading expert in this field, workplace fraud perpetrators resist a single profile, and their fraud is difficult to predict. But the best predictive characteristics for those who may commit fraud are employees with high personal debts or those who live beyond their means and who work in organizations that do not enforce clear lines of authority or proper procedures for transaction authorization. Financial personnel who refuse to take vacations is another red flag. The ACFE study found that the most likely locations for the kinds of fraud striking nonprofits (skimming, billing schemes, and cash larceny) are accounting per-

What is our organization's approach to transparency, and is there an open door for whistle-blowers? Is there a culture of asking questions and rewarding people for having asked them?

sonnel, followed by executive and upper management and sales.

So what should organizations do? First, every economic entity needs property insurance and, depending on size, may also need to buy employee dishonesty coverage to protect against fraud—usually when required by a governmental funding source or after a loss has been incurred. For this coverage, insurance companies may require nonprofit policy holders to ensure that bank accounts are reconciled by someone not authorized to deposit or withdraw. Second, officers and employees should be required to take annual vacations of at least five consecutive business days or the organization should be required to have an annual audit. Insurers want to see good business practices that in themselves help prevent fraud—and lower claims.

Prior to Consideration of Fraud in a Financial Statement Audit (SAS No. 99), auditing standards did not encourage fraud-detection procedures. With SAS No. 99, there is a better opportunity for the annual audit process to detect at least major fraud activity, but it is not a guarantee. Certainly, the external audit cannot be relied on as the sole detection or prevention strategy. Of the 58 nonprofit cases examined in this study, only 10 percent were discovered during the annual audit. Nonprofit audit committees and boards must install methods to reduce the risk of loss from fraud. Some key recommendations to reduce the risk of fraud as set forth by Floch (2004) and R. Wells (2005) include the following:<sup>2</sup>

- Require background checks for all employees with access to cash and other liquid assets.
- Check the Web sites of various state charity offices for advisories and final judgments identifying individuals or fundraising firms involved with fraud as well as for more general advice on fraud prevention and detection.
- Consider insurance or bonding for all employees with access to cash or other assets.
- Make it easy for employees, vendors, customers, and others to confidentially report suspected fraud or abuses.
- Periodically review internal controls to ensure that they can detect more than just small-scale fraud. Managers, executives, and others in positions of power have opportunities to bypass internal controls and perpetrate major fraud. When certified fraud examiners were asked on

a scale of one (ineffective) to five (effective) about the rankings of fraud prevention measures, strong internal controls ranked higher (3.66) than any other measure. ACFE recommends the use of its Fraud Prevention Check-Up to help identify and fix problems before it is too late (see [www.acfe.com/fraud/check.asp](http://www.acfe.com/fraud/check.asp)), and it's an excellent resource for nonprofit audit committees. (For more, see "Assessing Fraud Risk." on page 33.)

## Conclusion

While the ACFE sample is too small to draw firm conclusions about fraud in the nonprofit sector, it does highlight some interesting questions and challenges for nonprofits. Since it appears that audits and audit processes do not detect a great deal of fraud, and considering that many nonprofits do not conduct audits (while many others fall below the averages presented in this small sample), much of the burden for detecting fraud falls on informal systems that form the core of organizations' operations.

There are some questions that organizations should ask themselves: What is our organization's approach to transparency, and is there an open door for whistle-blowers? Is there a culture of asking questions and rewarding people for having asked them? Is the board and executive leadership engaged in a way that ensures that difficult questions are asked before fraud surfaces on its own? For organizations that do not conduct an audit, are policies in place to ensure good accountability? (For more on this topic, see *NPQ* Spring 2007, "Absent the Audit: How Small Nonprofits Can Demonstrate Accountability Without One" by Jeanne Bell and Steve Zimmerman.)

## ENDNOTES

1. Joseph T. Wells, *Principles of Fraud Examination*. New Jersey: John Wiley & Sons Inc., 2005.
2. Julie L. Floch, "Audits, Standards, and Integrity in Nonprofit Organizations. *The Practical Accountant*, Vol. 37, August 2004. Wells, R. Senate hearing probes tax abuse by charity groups. *Wall Street Journal*, 245 (67), p. D2, April 6, 2005.

Has your organization ever experienced fraud? How was it committed, discovered, and managed? Share your experience at [feedback@npqmag.org](mailto:feedback@npqmag.org). Reprints of this article may be ordered from <http://store.nonprofit>

## Assessing Fraud Risk

by Joseph T. Wells and John D. Gill

Every organization faces some risk of fraud from within. Fraud exposure can be classified into three broad categories: asset misappropriation, corruption and fraudulent financial statements.

Answering the following 15 questions is a good starting point for sizing up a company's vulnerability to fraud and creating an action plan for lessening the risks. The questions are based on information from the 2007 edition of the Fraud Examiners Manual published by the Association of Certified Fraud Examiners.

**1. Do one or two key employees appear to dominate the company?**

If control is centered in the hands of a few key employees, those individuals should be under heightened scrutiny for compliance with internal controls and other policies and procedures.

**2. Do any key employees appear to have a close association with vendors?**

Employees with a close relationship to a vendor should be prohibited from approving transactions with that vendor. Alternatively, transactions between these parties should be reviewed on a regular basis for compliance with internal controls.

**3. Do any key employees have outside business interests that might conflict with their job duties?**

Take the example of a 32-year-old sales representative who started a software company using his employer's time, equipment and facilities. The software company he worked for discovered that the employee demonstrated his own products to the company's customers. Ultimately, the employee diverted \$500,000 in business away from his employer.

The example illustrates why key employees should provide annual financial disclosures that list outside business interests. Many companies, particularly publicly traded companies, require such disclosures. Interests that conflict with the organization's interests should be prohibited. Organizations should implement an explicit policy that forbids employee business activities that directly compete with the operations of the organization.

Employees who have something to hide may lie or omit key facts on the disclosure form, but requiring the step still has advantages, such as making it easier to fire workers who fail to reveal potential conflicts. If an employer can show that an employee had such an interest and failed to disclose it on an annual reporting form, the employee can be fired simply for failing to follow company policy.

**4. Does the organization conduct pre-employment background checks to identify previous dishonest or unethical behavior?**

Organizations should conduct pre-employment background checks before offering employment to any key applicant. The scope of a background check varies by position, but a general list to consider includes: criminal records and convictions; Social Security number verification; credit history; previous employment; employment references; personal references; education verification; professional license verification; driver's license verification and driving history check; and civil records and judgments. Employers should ensure that legal requirements are met for the use of and access to the information.

For companies that have failed to do background checks, post-hire screenings may be appropriate in some cases, but should be conducted on the advice of legal counsel. A number of legal issues come into play when employers consider screening workers who are already on the job.

**5. Does the organization educate employees about the importance of ethics and anti-fraud programs?**

All employees should receive training on the ethics and anti-fraud policies of the organization. The employees should sign an acknowledgement that they have received the training and understand the policies.

**6. Does the organization provide an anonymous way to report suspected violations of the ethics and anti-fraud policies?**

Organizations should provide employees, vendors and customers with a confidential system for reporting suspected violations of the ethics and anti-fraud policies. According to the 2006 ACFE Report to the Nation on Occupational Fraud and Abuse, frauds are most commonly detected by a tip. The greatest percentage of those tips comes from employees of the victim organization.

In one instance, an anonymous tip received by a fraud hotline thwarted a fraud scheme that had drained approximately \$580,000 from a business. The caller reported that the company's accounts payable manager was approving fictitious invoices from his own outside company. The tip clued in company management to the scheme and brought an abrupt end to the manager's windfall. The fraudster was terminated and arrested. The company ultimately recouped most of its losses.

**7. Is job or assignment rotation mandatory for employees who handle cash receipts and accounting duties?**

Job or assignment rotation should be considered for employees who work with cash receipts and accounting duties. The frequency of the

rotation depends on the individual's responsibilities and the number of people available for the revolving duties.

**8. Has the company established positive pay controls with its bank by supplying the bank with a daily list of checks issued and authorized for payment?**

One method for a company to help prevent check fraud is to establish positive pay controls by supplying its banks with a daily list of checks issued and authorized for payment. Banks verify items presented for payment against the company's list and reject items that don't appear on the list.

The use of those controls foiled a fraud attempt by an employee and his accomplice, who worked for a check-printing company. The accomplice printed blank checks with the account number belonging to the perpetrator's employer. The perpetrator then wrote more than \$100,000 worth of forgeries on the counterfeit checks.

When the checks were presented to the bank for payment, they did not appear on the organization's list of expected payments. The bank refused to cash them. The organization was notified, and the fraudsters were arrested.

**9. Are refunds, voids and discounts evaluated on a routine basis to identify patterns of activity among employees, departments, shifts or merchandise?**

Companies should routinely evaluate those transactions to search for patterns of activity that might signal fraud.

**10. Are purchasing and receiving functions separate from invoice processing, accounts payable and general ledger functions?**

Segregation of duties is an important control. The failure to segregate these duties allowed one large, publicly traded company to be duped by a member of its managerial staff. The individual managed a remote location of the company and was authorized to order supplies and approve vendor invoices for payment. For more than a year, the manager routinely added personal items and supplies for his own business to orders made on behalf of his employer. The orders often included a strange mix of items. For instance, technical supplies and home furnishings were purchased in the same order.

In addition to ordering personal items, the employee changed the delivery address for certain supplies so they were shipped directly to his home or side business. Because the manager was in a position to approve his own purchases, he could get away with such blatantly obvious frauds. The scheme cost his employer approximately \$300,000 in unnecessary purchases.

**11. Is the employee payroll list periodically reviewed for duplicate or missing Social Security numbers?**

Organizations should check the employee payroll list periodically for

duplicate or missing Social Security numbers that may indicate a ghost employee or overlapping payments to current employees.

**12. Are there policies and procedures addressing the identification, classification and handling of proprietary information?**

To help prevent the theft and misuse of intellectual property, the company should implement policies and procedures addressing the identification, classification and handling of proprietary information.

**13. Do employees who have access to proprietary information sign nondisclosure agreements?**

All employees who have access to proprietary information should sign nondisclosure agreements. It is easier to sue for breach of a nondisclosure agreement than it is to sue for theft of information. Nondisclosure agreements afford companies legal options for the use of nonpublic information, not simply for information that is considered a trade secret.

In most states, companies without nondisclosure agreements may be limited to suing for theft of trade secret information.

**14. Is there a company policy that addresses the receipt of gifts, discounts and services offered by a supplier or customer?**

Organizations should implement a policy that sets ground rules about employees accepting gifts, discounts and services offered by a supplier or customer. If no explicit policy is in place, employees may find themselves in ambiguous situations without clear ethical guidelines.

For example, a city commissioner negotiated a land development deal with a group of private investors. After the deal was approved, the commissioner and his wife were rewarded by one of the investors with an all-expenses-paid international vacation.

While the promise of the trip may have influenced the commissioner's negotiations, this would be difficult to prove. However, had a clear policy regarding the receipt of gifts been implemented and enforced, the commissioner would have known that accepting the free vacation was a violation of the rules. The ambiguity of the situation would have been avoided.

**15. Are the organization's financial goals and objectives realistic?**

Closely monitor compliance with internal controls over financial reporting if the financial goals and objectives appear to be unrealistic. Establish realistic financial goals and objectives for the organization. Common justifications for financial statement fraud include a desire to obtain bonuses linked to goals or frustration with objectives that were unachievable through normal means.

---

Joseph T. Wells, CPA, CFE, is founder and chairman of the Association of Certified Fraud Examiners and a contributing editor to the JofA. His e-mail address is [jwells@acfe.com](mailto:jwells@acfe.com). John D. Gill, J.D., CFE, is research director for the Association