Fraud in the NONprofit sector?

You bet.

By Thomas Buckhoff, CPA, and Abbie Gail Parham, CMA, CFM, CPA

Because their mandate is so noble, many nonprofit organizations (NPOs) mistakenly assume that their employees and volunteers wouldn't steal from them. What coldhearted person would steal money donated to grant wishes for terminally ill children or make off with funds pegged to important research? Misguided beliefs like these often influence accountants and auditors of NPOs and small charities to be less diligent than their counterparts in large for-profit entities in setting up controls for safeguarding cash. As a result of these lax controls, many NPOs become breeding grounds for fraudulent activity.

Consider the following case examples:

- A former program administrator of the Carnegie Institution of Washington, which conducts scientific research across several disciplines, pleaded guilty to embezzling $202,000 earmarked to help public-school teachers become better versed in science.
- The founder of the Thornton Kidney Research Foundation pleaded guilty to mail and wire fraud and was ordered to pay $644,000 in restitution. His transgressions also got him eight years in federal prison.
- The former CEO of the Indianhead Community Action Agency, which helps the poor find housing and offers them literacy training, was charged with forging checks in excess of $1 million.
- A former president of Goodwill Industries was indicted on federal charges that he stole more than $800,000 from the charity by wiring money to overseas bank accounts. Since then, a financial controller of Goodwill Industries was charged with embezzling nearly $400,000.
- A former accounts payable clerk for NorthBay Healthcare Group, a not-for-profit organization that operates hospitals and clinics in Vacaville and Fairfield, Calif., pleaded guilty to computer fraud. She used her computer to gain unauthorized access to the company's accounting software and issue checks payable to herself and others, resulting in the theft of at least $875,000.
- An internal investigation by Oxfam International, a relief organization, uncovered fraudulent expenditures of $22,000. Oxfam paid for relief supplies that were never delivered to a province in Indonesia following the 2004 tsunamis in South Asia. Most of the funds were recovered, and 22 employees are facing disciplinary action, including possible dismissal.

A Growing Problem

According to the *2008 Report to the Nation on Occupational Fraud and Abuse* by the Association of Certified Fraud Examiners (ACFE), occupational fraud and abuse costs U.S. organizations roughly $994 billion annually, or about 7% of total revenues. Results of other surveys underscore an emergent problem. In 2006, KPMG conducted a fraud survey of 459 public companies, nonprofit organizations, and state and federal government agencies. Some 75% of the respondents reported that their organizations had suffered losses because of employee fraud during the past year, with the average loss coming in at $464,000. And (surprise!) workers at foreign charities and nonprofits aren't immune from corruption, either. In its 2008 fraud survey, BDO Kendalls, a worldwide network of public accounting firms, received 384 responses from not-for-profit organizations based in Australia and New Zealand. Major findings included:

- The typical fraudster was in his or her 40s and was a paid nonaccounting employee.
- The average fraud loss was $45,527.
- About 92% of fraud was committed by paid employees and only 8% by unpaid volunteers.
- Cash theft and kickbacks/bribery were the most common types of fraud reported.
- The largest number of fraud incidents was reported in organizations with no volunteers.

As these statistics and case examples illustrate, small charities and NPOs aren't immune from this disturbing trend toward greater employee dishonesty. It's important to note, however, that the results of all fraud surveys reflect incidents that were actually *discovered*, which some fraud experts estimate comprise less than half of all fraud being perpetrated. Thus, most employee fraud goes undetected. By whatever measure, this type of deception has become increasingly widespread and is an enormous and intolerable financial drain on our society.

Fraud Prevention and Detection

Preventing fraud in NPOs—or in any business, for that matter—is a two-step process: (1) conduct employee background checks, and (2) minimize opportunities for internal theft. Fraud experts estimate that NPOs can prevent about 80% of fraud by effectively screening prospective employees and volunteers. Those with criminal backgrounds and/or who misrepresent themselves on their employment applications are most likely to commit fraud. Case in point: According to an Aug. 7, 2003, article, "Fighting Charity Fraud," in *The Chronicle of Philanthropy*, Steven Mason, the father of three young children and an overtly religious man, was criminally convicted for unemployment compensation fraud and receiving stolen property. Subsequently, Workforce Central Florida, a nonprofit job-placement program, hired Mason as finance director. Mason stole $172,000. Impressed by his experience as finance director for Workforce Central Florida, and with no knowledge of his past, United Arts of Central Florida hired Mason as finance director. He then allegedly stole $148,000 from United Arts. Neither of these two NPOs conducted background checks on Mason before hiring him; they presumably considered the nominal cost of performing such checks to be an unnecessary expense. Both organizations learned from

their mistakes and, not surprisingly, now conduct background checks on every prospective employee. (For more information, see http://philanthropy.com/free/articles/v15/i20/20002901.htm.)

How can your organization minimize opportunities for internal theft? The most effective way is to implement and adhere to a good system of internal controls. The three primary objectives of such a system include: (1) safeguarding the organization's assets, (2) ensuring the accuracy and timeliness of financial information, and (3) encouraging compliance with organizational policies, procedures, laws, and regulations. An effective internal control system should include the following five procedures:

1. Proper Authorization and Segregation of Duties. The same employee shouldn't perform more than one of the following three job functions: authorization, custody of assets, and recordkeeping. For example, Steven Mason exploited his position as finance director by writing checks to himself (an authorization function), signing the checks (a custody-of-assets function), and recording the disbursement of funds as "operating support" for a local arts group (a recordkeeping function). Of course, employees performing different functions can collude to commit fraud, but such situations are rare. The 2008 BDO Kendalls fraud survey indicated that collusion occurred in only 19% of reported cases. Thus, the risk of fraud can be greatly reduced by adequately segregating job functions to make it difficult for one person to act alone.

2. Adequate Documents and Records. Documentation and records provide a paper trail that helps organizations keep track of their limited resources. Charities and companies with poor tracking systems tend to be ripe for fraud. Understandably, employees are less inclined to steal if they're made aware that the organization carefully and precisely documents all of its income and expenses. Ideally, all NPOs should maintain source documentation for all cash receipts and cash disbursements. A source document should be an original document that includes the date, amount, and business-related purpose of the transaction. Common examples of source documents include, but aren't limited to, vendor invoices, sales receipts for purchases made, cash register tapes, and bank deposit tickets, including copies of all checks received from donors. The absence of adequate source documentation can be a red flag that an insider is defrauding the organization.

3. Physical Safeguards. Organizations (for-profit and nonprofit alike) can minimize opportunities for misuse or theft by limiting access to physical assets and accounting records by unauthorized personnel. Such safeguards include locked cash registers and storerooms, electronic passwords, fireproof safes, fences around buildings, and secure storage lots for equipment and materials. Special fund-raising events are prime targets for employees and volunteers to commit fraud. These events usually involve large volumes of cash that many individuals may handle with little or no control procedures in place. If it hasn't already, your organization should implement the following physical safeguards:

- Use cash registers and/or locked boxes, and limit access to both.
- Deposit cash in the bank the same day cash was received, if possible.
- Require passwords to access the computerized accounting system, and limit access to them.

4. Electronic Controls. Protecting confidential information isn't only a business requirement—it's often a *legal* requirement. Employees can breach confidentiality by simply allowing someone to use their password to access company data. From there, unauthorized users can alter, delete, or steal information. Moreover, hackers pose threats from outside the organization and can gain access to company data through electronic trickery like "masquerading" and "piggybacking."

What can you do to mitigate the risk of security violations and loss of data? The first step is to implement proper access-control mechanisms, beyond just usernames and passwords, so that only authorized persons are able to view data, perform tasks, or both. This probably will mean creating several levels of security and, therefore, several levels of users. "Data masking" is a method of hiding sensitive information within a database so that it can't be leaked to others. Encryption technology, which allows only authorized users to access ("decrypt") certain information, is becoming increasingly important for companies that allow employees to use laptops, CDs, and USB keys that contain confidential data. Other strategies include maintaining antivirus protection

to detect threats and crafting policies to limit and/or control Internet use to help prevent access to infected websites. All of these strategies will help protect your company from accidental loss or deliberate theft, as well as secure the data so it can't be read if it's lost or stolen.

5. Independent Checks. The notion underlying independent checks is that if employees know that their activities are being monitored, the perceived opportunity to commit fraud is reduced. For example, when an independent manager (one with no access to donated cash) compares the cash receipts log to what was deposited in the bank, the manager is making sure that all cash received actually was deposited into the bank. Such independent checks not only guard against employee fraud but also uncover honest mistakes. But the biggest concern with not-for-profit organizations is that incoming cash donations won't be logged in but will instead be diverted into the pockets of dishonest employees or volunteers. The following controls over cash receipts should be implemented to minimize losses:

- Create some kind of estimate regarding the amount of cash that, according to the budget, should have been received, and reconcile it to the amount of cash actually received.
- Create a record of cash actually received, and reconcile it to deposits on the monthly bank statements.
- Require at least two people to be present whenever cash is received.
- In lieu of cash donations, request that donors pay by check or by credit or debit card.

Few people who steal expect to be caught and punished. Thus, an effective way to prevent fraud is to make employees *think* they'll be caught and punished if they steal. Instilling this "perception of detection" in employees' minds is the single most effective way to prevent fraudulent activity. One way to send a clear message to employees and volunteers is by having a written policy stating the organization's stand and how it will deal with fraud perpetrators. Another strong deterrent: Install security cameras in areas where cash is handled. A less-expensive but perhaps equally effective option would be to conduct "surprise" audits of cash accounts since staffers and volunteers won't have time to cover their tracks. Smaller companies especially should have a policy of job rotation and enforced annual leave since many frauds require the person to maintain continuous, manual intervention.

Governance Issues

Recent accounting scandals have focused attention on corporate governance and directors' duties and responsibilities. Directors of not-for-profit organizations are legally bound by the fiduciary duties of care, loyalty, and obedience. The *duty of care*—to act as an ordinarily prudent person would under similar circumstances—requires that directors be informed and make decisions based on facts and reliable information. The *duty of loyalty* requires directors to use fairness, good faith, and honesty in their actions. It requires a director to act in a manner believed to be in the best interests of the corporation without considering any personal gain. Finally, the *duty of obedience* requires directors to carry out the mission of the organization while, at the same time, assuring that board policies and decisions comply with the law. In short, directors must be committed to the organizations they serve.

Adhering to these duties establishes high standards of accountability. NPOs are accountable to a number of groups, including state attorneys general and the Internal Revenue Service (IRS). As protectors of the public interest, state attorneys general oversee charitable organizations by investigating fraud allegations involving nonprofits and monitoring compliance with a state's fund-raising laws. The IRS is responsible for monitoring tax-exempt status and enforcing tax compliance for qualified charitable organizations.

Directors and officers—as well as corporate accountants and auditors—have a fiduciary duty to ensure that all of the donations received are used to carry out the NPO's charitable mandate. This can be accomplished by implementing and adhering to an internal control system that both minimizes opportunities to commit fraud and maximizes the probability that fraudulent acts will be detected early. Such a system requires the organization to conduct background checks on all employees and volunteers, establish controls for safeguarding cash receipts and disbursements, and demonstrate its commitment to a fraud-free environment by terminating and/or prosecuting those who exploit the organization for personal gain. **SF**

Thomas Buckhoff, CPA, Ph.D., is an associate professor of forensic accounting and fraud examination in Georgia Southern University's College of Business Administration. You can reach him at (912) 478-7142 or tbuckhoff@georgiasouthern.edu.

Abbie Gail Parham, CMA, CFM, CPA, is an assistant professor of accounting in Georgia Southern University's College of Business Administration. You can reach Abbie Gail at (912) 478-5037 or aparham@georgiasouthern.edu.