



# Preventing Employee Theft

## *Tips to minimize your risk of loss*

by Kathryn M. Vanden Berk

I have been amazed by how many incidents of nonprofit employee theft or fraud have been reported in the past few months in the *Chronicle of Philanthropy*. A recent article that caught my eye involved a trusted long-term employee who used access to the agency's expense reimbursement system to steal \$9,000.<sup>1</sup>

The *Chronicle* noted that a trusted employee is the most likely operator, since you wouldn't put someone you don't trust in a position where this could happen. One expert reported that 15 percent of employees would never steal, regardless of the opportunities presented. Another 15 percent will always steal if they think they can get away with it, and the 70 percent in the middle can succumb to temptation if there is motive, opportunity, and some sort of internal justification.<sup>2</sup>

Theft and fraud cases almost always follow a lapse on the employer's part. Often something that could have been done to prevent the theft was not done, or obvious opportunities for fraud were overlooked because the person had been at the organization for many years, or was beloved by most.

We will no doubt discover more nonprofit theft in coming years, as the new Internal Revenue Service (IRS) Form 990 creates a more transparent reporting system and computers allow questionable transactions to be tracked in more sophisticated ways. In the meantime, here is what you need to do to prevent theft or fraud, as well as advice for what to do if you discover that it has already occurred.

The most common forms of theft and fraud involve:

- receiving kickbacks from vendors,
- purchasing supplies or services from fictitious companies,
- making unauthorized purchases,
- overcharging for goods and services,
- creating false invoices or engaging in other fraudulent billing practices,
- overpaying employees or writing payroll checks to nonexistent employees,
- stealing inventory or other company property,
- forging checks or stealing cash, and
- inflating expense accounts.

### Establish a Control Environment

The best way to avoid employee theft is to adhere to the ordinary controls that have been developed over the years to rein in employee errors, mismanagement, and fraud.<sup>3</sup> A good internal control policy should accomplish four general objectives: authorization, recording, safeguarding, and accountability.

**Authorizations and Approvals.** The first goal is to ensure that transactions conform to agency intentions. *Authorizations* are done in advance and may be general (relating to all transactions) or specific to a single transaction. *Approvals* come after the transaction has occurred and ensure that a completed or partly completed transaction meets specified requirements. Authorizations and approvals should always be done by a superior, and it is especially important that neither task revert to an automatic rubber stamping.

**Recording.** Recording is intended to ensure that authorized transactions are recorded (1) in the proper accounting periods, (2) at the correct amounts, and (3) for the appropriate accounts. Recording controls focus on documents (purchase orders, shipping records, and sales invoices) and books of account (the general ledger, subsidiary ledgers, and journals).

**Safeguarding.** Safeguarding is meant to ensure that access is limited to authorized persons under proper controls. You control access to physical assets by having proper storage facilities, keeping updated asset inventories, and establishing policies and procedures for those who access computers and other valuable agency properties.

**Accountability.** Accountability processes are intended to ensure that preventive controls are functioning as intended and, if the preventive controls are breached and a fraud is committed, that it will be detected before harm is done. Controls generally involve some form of comparison: comparing asset records with the assets themselves, accounting records with the supporting documentation, or general ledger accounts with subsidiary ledgers and journals.

Processes to safeguard nonprofit assets involve segregation of duties. Your accounting or auditing firm should be providing you with a good basic policy. It is a good idea to revisit that policy from time to time in order to ensure that it continues to meet your needs (I suggest an internal controls checklist, a sample of which is available at [magazine.alliance1.org](http://magazine.alliance1.org)).

*Continued on page 46*

Your goal is to create a “control environment,” an infrastructure and ethos that reinforces the theme that everyone is involved in reducing the risk of loss. A control environment is marked by a top-down culture of competence and accountability. Standard policies that demonstrate a policy of no tolerance toward theft include:

- rigorous background checking process of all new hires,
- emphasis on control issues during orientation,
- obtaining surety bonds for employees who handle money or other valuable assets,
- a written code of ethics that is clearly enforced by your disciplinary process,
- a whistleblower hotline or open door policy,
- an audit process that is supervised by your board of directors, and
- leaders who clearly “walk the talk.”

### If a Loss Occurs

Every case is different. There are a number of actions that must be taken, and others that can or should be taken depending upon the type of loss. Here are some suggestions:

**Report to Your Board.** No matter what the loss, bring the matter to your board chair or president and let him or her decide whether to include other board members in evaluating the situation and planning your response.

**File a Police Report.** File a report with your local law enforcement agency and seek assistance with your investigation if that would help. They can help you connect with prosecutors if the loss involves violation of criminal statutes.

**File an Insurance Claim.** Review your policy’s notice requirements and file a claim within the prescribed time limits.

**Prepare a Crisis Management Plan.** The publicity that follows a loss can cripple the organization if it appears that management was slack. Be sure to work with your public relations staff or consultants to establish and implement a public relations plan to blunt public criticism and work behind the scenes with donors.

**Conduct a Forensic Audit.** Because there are legal consequences, you may

want to conduct a forensic audit. This will ensure that the activities are documented for future legal review.

#### Report to State Charity Regulators.

If your state has a department of government that is responsible for charitable solicitation, its charity regulators may assist with your investigation.

**Report to State Professional Licensing Boards.** If the offending individual is a licensed professional, report the incident to his or her professional licensing board.

**File Reports with the IRS.** The IRS considers theft loss to be a casualty loss rather than income to the offending individual, since income is given for services performed rather than assets taken.<sup>4</sup> If the matter can be described as an excess benefit transaction, you may be required to report it on your Form 990 Information Return for the relevant year.<sup>5</sup> Finally, the IRS also has a fraud unit in its Dallas office that is specific to exempt organizations.<sup>6</sup>

#### File Reports with the Post Office.

If the loss involved use of mail, notify your local postmaster or call the Postal Inspection Service Criminal Investigation Service Center.<sup>7</sup>

Whenever there is a loss due to theft or fraud, be sure to work closely with your accountants and legal counsel to be sure you have covered all bases. You certainly want to be sure to plug the holes that allowed the incident to occur in the first place.

The best outcome is a return of the assets, punishment of the thief, and no loss of reputation. The most important information to disseminate is that you have already identified the problem, reported it to the proper authorities, and taken steps to prevent future losses. ■

#### ENDNOTES

1. Frazier, Eric, “Fighting Nonprofit Fraud: Charities need to tighten controls against theft in a tough economy,” *The Chronicle of Philanthropy*, May 21, 2009.
2. This was revealed during a Sept. 23, 2004 radio interview between John Dini and Jim Blasingame. You can hear the audio at [smallbusinessadvocate.com/small-business-interviews/john-dini-1857](http://smallbusinessadvocate.com/small-business-interviews/john-dini-1857).
3. These three terms have specific meanings, each of which describes a specific kind of loss exposure. Error involves simple mistakes: a number is transposed, a date is incorrect. Mismanagement involves incompetence: the operator doesn’t know how to enter a transaction correctly. Fraud involves intentional activity.

4. Losses that can be considered income can be reported on a Form 1099-MISC. Casualty losses are claimed on Form 4684 Casualties and Thefts as an “unreported income event.” You can find more about filing a Form 4684 in IRS Publication 584B, *Business Casualty, Disaster and Theft Loss Workbook*.
5. The IRS considers an excess benefit transaction (EBT) to have occurred at the time of the taking, whether or not the loss is recovered. You will need to evaluate the potential downside of reporting an EBT on your Form 990, as this is a public document. See more about EBTs on the IRS website at [irs.gov/charities](http://irs.gov/charities).
6. You may access the IRS Exempt Organization Fraud Unit by filing a notice with your regional IRS office, or by going directly to the exempt organizations unit in Dallas. The hotline is 800-829-0433 and the mailing address is IRS—EO Classification, 4910 DAL, 1100 Commerce St., Dallas TX 75242-1198. Download and complete Form 3949-A Information Referral so that you have all relevant facts covered in your report.
7. The United States Postal Service fraud hotline is 800-FRAUD IS (1-800-372-8347) or online at [usps.com/postalinspectors](http://usps.com/postalinspectors).

#### DISCLAIMER

This article has been prepared to convey general information on a topic of interest to the boards and executive staff of nonprofit human service organizations. Although prepared by an attorney, it should not be used as a substitute for legal counseling in specific situations. Readers should not act upon the information contained in this article without professional guidance.



*Kathryn Vanden Berk practiced law for nine years before serving as the president of two residential treatment centers for children. Now practicing in Chicago, she focuses on nonprofit start-ups,*

*corporate and tax law, and employment issues. She serves as adjunct faculty at several Chicago universities, and is a member of the Advisory Board of the Axelson Center for Nonprofit Management at North Park University. She authored a handbook on starting nonprofits that is available from the Nonprofit Financial Center, Chicago, and a chapter in the Illinois attorney’s handbook Not-for-Profit Corporations, 2004 Ed., Illinois Institute of Continuing Legal Education. In 2004 she authored Retooling Employment Standards for the Future, a publication of the First Nonprofit Educational Foundation, Chicago. She can be reached at 312-442-9076 or at [info@beavandenberk.com](mailto:info@beavandenberk.com).*