Risk Control Bulletin

Fraud at Not-For-Profits: Internal Controls Mitigate Risk

CNA
We can show you more.®

RISK CONTROL

The following incidents are just a few examples of fraudulent activity that have occurred in not-for-profit organizations in recent years:

- A former CEO of a not-for-profit organization serving the mentally disabled pleads guilty to embezzling over $600,000.[1]
- A former executive director of a charity assisting low-income individuals admits to stealing $900,000 from the organization.[2]
- An employee of a major metropolitan arts center steals an estimated $1.44 million over a five-year period by submitting fake invoices.[3]

As these situations illustrate, no organization is immune from fraud, regardless of size, purpose or business model. In fact, not-for-profit organizations may be more susceptible to theft and embezzlement because of their culture of trust, where it is often assumed that directors and staff are solely motivated by the organization's mission. However, the same temptations exist in the philanthropic sector as among for-profit enterprises. Moreover, economic conditions, staff cutbacks and consequent decreased supervision may combine to make white-collar crime more likely.

Extent and Types of Criminal Activity

A 2013 Washington Post investigation into Internal Revenue Service filings revealed that more than a thousand not-for-profit organizations had reported a "significant diversion" of assets due to theft and fraud, with total losses amounting to hundreds of millions of dollars.[4] Fraud in the not-for-profit sector is even more prevalent than these numbers suggest, as only larger entities are required to file IRS Form 990. In addition, those that file need only report diversions greater than $250,000 or that constitute more than 5 percent of the organization's annual gross receipts or assets.

In a 2012 research study, Marquet International reported that not-for-profit entities comprise one-sixth of major embezzlements, behind only financial services and government sectors. Another study also published in 2012 by the Association of Certified Fraud Examiners (ACFE) found that, on average, about 5 percent of organizational revenues is lost to internal fraud.[5]

Some of the most common types of fraud committed against not-for-profits include:

- *Forging checks* made out to cash or oneself, or used for personal purchases.
- *Pocketing cash receipts* meant for deposit into institutional accounts.
- *Issuing extra paychecks* or bonus payroll checks to oneself.
- *Padding expense reports* with inflated, nonexistent or illegitimate charges.
- *Submitting false invoices* from phony or legitimate vendors.
- *Abusing an organizational credit card account* by making individual purchases.
- *Electronically transferring organizational funds* to personal accounts or vendors for private purchases.
- *Stealing organizational equipment*, inventory or supplies.[6]

General Risk Control Tips

The scenarios cited above underscore not-for-profit organizations' need to develop and implement sound financial controls to prevent fraudulent activity. Often, the individuals who commit these crimes serve in positions of trust and may be considered "above reproach." For this reason, a watchful eye should be kept on all financial activities, and to apply policies and controls impartially throughout the organization, without exception.

Below are some suggestions designed to help the leadership of not-for-profits enhance internal controls and minimize exposure to fraud:

Encourage ethical behavior. Clearly written ethics policies are important to preventing theft, but they must be supported by periodic training and frequent reminders of organizational rules and expectations.

Establish a reliable reporting program. The core and substance of any ethics policy are its reporting procedures, as internal scams are most commonly discovered via employee tips.[7] The process should be clear, simple and

---

1 "Ex-head of N.Y. Disability Nonprofit Admits to $600,000 Theft." Philanthropy Today, June 15, 2012. Available here.

2 *Philanthropy Today*, 8/1/12. Available here.

3 "Fraud Suspected in Atlanta Arts Center's $1.4-million Loss." *Philanthropy Today*, November 29, 1012. Available here.

4 Stephens, J. and Flaherty, M.P. "Inside the Hidden World of Thefts, Scams and Phantom Purchases at the Nation's Nonprofits." *Washington Post*, October 26, 2013. Available here.

5 *2012 Report to the Nations on Occupational Fraud and Abuse*. Key findings and highlights are available at http://www.acfe.com/rttn.aspx.

6 *The 2012 Marquet Report on Embezzlement*,May 14, 2013. Available here.

7 ACFE's *Report to the Nations on Occupational Fraud and Abuse: 2012 Global Fraud Study*, page 14. Available here.

protective of informants. Consider permitting anonymous reporting, in order to encourage participation and shield staff members from possible retaliation.

Rotate job duties. Ensure that no single individual is always and solely responsible for a specific task, as employees cannot maintain full control of a criminal scheme if their job duties change periodically. Cross-training and job rotation thus represent the key to detecting and deterring fraud.

Enforce a mandatory vacation policy. Staff members who commit fraud often refuse to make use of their earned time off, in order to prevent others from noticing their illicit activities. By requiring periodic breaks, leadership can disrupt fraudulent operations and significantly enhance the likelihood of discovery.

Prohibit executives or managers from overriding internal controls. To prevent potential abuses of power, consider implementing a program to monitor and review managerial overrides of financial controls and standard procedures.

Conduct both periodic and unscheduled audits. In addition to regularly scheduled audits, periodically perform unscheduled inspections of financial records and inventory, in order to prevent wayward staff from attempting to destroy, alter or conceal potentially incriminating documents. A policy of unscheduled audits and inspections also serves to deter white collar crime.

Treat employees with respect. A positive, fair-minded, respectful work environment reduces the risk of internal fraud, as staff members who consider themselves mistreated, under-appreciated or under-rewarded are more apt to feel justified in stealing from their employer.

Enhancing Financial and Payroll Management

Some internal embezzlement schemes involve creating phony vendor accounts or fictitious employees and "paying" them with organizational funds. By separating and monitoring certain functions, organizations make it considerably more difficult for employees to cover up embezzlement. Consider the following safeguards for cash receipts, cash disbursements, and payroll processes:

Separate cash receiving and processing functions. Assign the task of receiving and reviewing unopened checks and preparing bank deposits to an employee who is not involved in recording payments in the accounts receivable ledger, authorizing write-offs and adjustments to customer accounts, or regularly reconciling all bank statements. Any observed irregularities should be immediately reported to the bank.

Monitor bank activity. Review and evaluate all deposits and payments made, including payee names, payment amounts and authorizing signatures. Monitoring serves to both detect and deter fraud by sending a message that the organization is vigilant about its financial practices.

Segregate vendor order and approval functions. Assign the task of vendor set-up and vendor master file maintenance to an employee who is not involved in generating and authorizing cash disbursements to vendors.

Check vendor addresses and invoices. Periodically compare vendor addresses to employee addresses to see if any match. In addition, regularly audit invoices to ensure that billed products and services have been received.

Segregate payroll records and payroll processing functions. All changes made to employee payroll records should be approved and recorded by another staff member. Furthermore, employees who maintain payroll records should not be involved in approving, generating or distributing paychecks.

Require dual signatures on every check. Organizations can reduce the risk of forgery by requiring two signatures on all checks, as well as eliminating endorsement stamps and prohibiting the signing of blank checks. It is also advisable to have a high-ranking executive endorse checks over a certain amount.

Internal theft can result in significant harm to an organization's image and balance sheet, threatening its ability both to perform its mission and to raise funds. This makes it imperative that all not-for-profits implement a sound program to prevent fraud and to respond swiftly and effectively to any sign of questionable financial activities anywhere within the organization.